Firewall Aker

Manual de Configuração da Versão 5.1

- Introdução
- 1-0 Instalando o Firewall Aker
  - 1-1 Requisitos de hardware software
  - 1-2 Instalando o firewall
  - 1-3 Instalando a interface remota em plataformas Windows, Linux e FreeBSD
- 2-0 Utilizando a interface remota
  - 2-1 Iniciando a interface remota
  - 2-2 Finalizando a administração remota
  - 2-3 Mudando sua senha de usuário
  - 2-4 Visualizando informações da sessão
  - 2-5 Utilizando a ajuda on-line
- 3-0 Administrando usuários do firewall
  - 3-1 Utilizando a interface gráfica
  - 3-2 Utilizando a interface texto
- 4-0 Configurando os parâmetros do sistema
  - 4-1 Utilizando a interface gráfica
  - 4-2 Utilizando a interface texto
- 5-0 Cadastrando Entidades
  - 5-1 Planejando a instalação
  - 5-2 Cadastrando entidades utilizando a interface gráfica
  - 5-3 Utilizando a interface texto
  - 5-4 Assistente de Entidades
- 6-0 O Filtro de Estados
  - 6-1 Planejando a instalação
  - 6-2 Editando uma lista de regras usando a interface gráfica
  - 6-3 Trabalhando com Políticas de Filtragem
  - 6-4 Utilizando a interface texto
  - 6-5 Utilizando o assistente de regras
- 7-0 Configurando a Conversão de Endereços
  - 7-1 Planejando a instalação
  - 7-2 Utilizando a interface gráfica
  - 7-3 Utilizando a interface texto
  - 7-4 Utilizando o Assistente de NAT
- 8-0 Criando canais de criptografia
  - 8-1 Planejando a instalação
  - 8-2 Carregando certificados Aker-CDP
  - 8-3 Carregando certificados IPSEC
  - 8-4 Configurando canais Firewall-Firewall
  - 8-5 Utilizando a interface texto
- 9-0 Configurando criptografia Cliente-Firewall
  - 9-1 Planejando a Instalação
  - 9-2 Configurando o firewall utilizando a interface gráfica
  - 9-3 Configurando o firewall utilizando a interface texto
  - 9-4 Instalando o cliente de criptografia Aker

    - 9-5 Configurando o cliente de criptografia
- 10-0 Configurações do Secure Roaming
    - 10-1 Utilizando a interface gráfica
- 11-0 Integração dos módulos do Firewall
    - 11-1 O fluxo de pacotes no Firewall Aker
    - 11-2 Integração do filtro com a conversão de endereços
    - 11-3 Integração do filtro com a conversão e a criptografia
- 12-0 Configurando a Segurança
    - 12-1 Proteção contra SYN Flood
    - 12-2 Utilizando a interface gráfica para Proteção contra SYN Flood
    - 12-3 Proteção de Flood
    - 12-4 Utilizando a interface gráfica para Proteção de Flood
    - 12-5 Proteção Anti Spoofing
    - 12-6 Utilizando a interface gráfica para Anti Spoofing
    - 12-7 Sistema de Detecção de Intrusão (IDS)
    - 12-8 Configurando o suporte para o agente de detecção de intrusão
    - 12-9 Instalando o Plugin para agentes IDS no Windows NT
    - 12-10 Utilizando a interface texto - Syn Flood
    - 12-11 Utilizando a interface texto - Proteção de Flood
    - 12-12 Utilizando a interface texto - Anti Spoofing
    - 12-13 Utilizando a interface texto - IDS
- 13-0 Configurando as ações do sistema
    - 13-1 Utilizando a interface gráfica
    - 13-2 Utilizando a interface texto
- 14-0 Visualizando o log do sistema
    - 14-1 Utilizando a interface gráfica
    - 14-2 Formato e significado dos campos dos registros do log
    - 14-3 Utilizando a interface texto
- 15-0 Visualizando os eventos do sistema
    - 15-1 Utilizando a interface gráfica
    - 15-2 Formato e significado dos campos das mensagens de eventos
    - 15-3 Utilizando a interface texto
- 16-0 Visualizando estatísticas
    - 16-1 Utilizando a interface gráfica
    - 16-2 Utilizando a interface texto
- 17-0 Visualizando e removendo conexões
    - 17-1 Utilizando a interface gráfica
    - 17-2 Utilizando a interface texto
- 18-0 Trabalhando com proxies
    - 18-1 Planejando a instalação
    - 18-2 Instalando o agente de autenticação em plataformas Unix
    - 18-3 Instalando o agente de autenticação em Windows NT/2000
- 19-0 Configurando parâmetros de autenticação
    - 19-1 Utilizando a interface gráfica
    - 19-2 Utilizando a interface texto
- 20-0 Perfis de acesso de usuários
    - 20-1 Planejando a instalação
    - 20-2 Cadastrando perfis de acesso
    - 20-3 Associando usuários com perfis de acesso
- 21-0 O cliente de autenticação Aker

    - 21-1 Planejando a instalação
    - 21-2 Instalando o cliente de autenticação Aker
    - 21-3 Configurando o cliente de autenticação
    - 21-4 Visualizando e removendo usuários logados no firewall
    - 21-5 Utilizando a interface texto
- 22-0 Configurando o proxy SMTP
    - 22-1 Editando os parâmetros de um contexto SMTP
- 23-0 Configurando o proxy Telnet
    - 23-1 Editando os parâmetros de um contexto Telnet
- 24-0 Configurando o proxy FTP
    - 24-1 Editando os parâmetros de um contexto FTP
- 25-0 Configurando o proxy POP3
    - 25-1 Editando os parâmetros de um contexto POP3
- 26-0 Configurando o proxy WWW
    - 26-1 Planejando a instalação
    - 26-2 Editando os parâmetros do proxy WWW
- 27-0 Configurando o proxy SOCKS
    - 27-1 Planejando a instalação
    - 27-2 Editando os parâmetros do proxy SOCKS
- 28-0 Configurando o proxy RPC
    - 28-1 Editando os parâmetros de um contexto RPC
- 29-0 Utilizando as ferramentas da interface gráfica
    - 29-1 Chaves de ativação
    - 29-2 Salvar cópia de segurança
    - 29-3 Carregar cópia de segurança
    - 29-4 DNS Reverso
    - 29-5 Data e Hora
    - 29-6 Varredura de regras
    - 29-7 Relatórios
    - 29-8 Atualizações
    - 29-9 Configuração TCP/IP
    - 29-10 Reinicializar firewall
    - 29-11 Localizar entidades
    - 29-12 Janela de Alarmes
    - 29-13 Visualizando a rede graficamente
    - 29-14 Visualizando estatísticas do sistema
    - 29-15 Utilizando a interface texto nas Chaves de Ativação
    - 29-16 Utilizando a interface texto na Configuração TCP/IP
- 30-0 Configurando o Firewall em Cluster
    - 30-1 Planejando a Instalação
    - 30-2 Utilizando a interface texto
- 31-0 Arquivos do sistema e backup
    - 31-1 Arquivos do sistema
    - 31-2 Backup do Firewall
- 32-0 Firewall Aker Box
- Apêndice A - Mensagens do sistema
    - Mensagens do log do Firewall
    - Mensagens dos eventos do Firewall
- Apêndice B - Perguntas e respostas
- Apêndice C - Copyrights e Disclaimers

- Apêndice D - Novidades da versão 5.1

Introdução

Este é o manual do usuário da versão 5.1 do Firewall Aker. Nos próximos capítulos você aprenderá como configurar esta poderosa ferramenta de proteção à redes. Esta introdução tem como objetivo descrever a organização deste manual e tentar tornar sua leitura o mais simples e agradável possível.

Como está disposto este manual.

Este manual está organizado em vários capítulos. Cada capítulo mostrará um aspecto da configuração do produto e todas as informações relevantes ao aspecto tratado.

Todos os capítulos começam com uma introdução teórica sobre o tema a ser tratado seguido dos aspectos específicos de configuração do Firewall Aker. Juntamente com esta introdução teórica, alguns módulos possuem exemplos práticos do uso do serviço a ser configurado, em situações hipotéticas porém bastante próximas da realidade. Buscamos com isso tornar o entendimento das diversas variáveis de configuração o mais simples possível.

Recomendamos que este manual seja lido pelo menos uma vez por inteiro, na ordem apresentada. Posteriormente, se for necessário, pode-se usá-lo como fonte de referência (para facilitar seu uso como referência, os capítulos estão divididos em tópicos, com acesso imediato pelo índice principal. Desta forma, pode-se achar facilmente a informação desejada).

Em vários locais deste manual, aparecerá o símbolo seguido de uma frase escrita em letras vermelhas. Isto significa que a frase em questão é uma observação muito importante e deve ser totalmente entendida antes de se prosseguir com a leitura do capítulo.

Interface texto vs. Interface Gráfica

O Firewall Aker possui duas interfaces distintas para sua configuração: uma interface gráfica remota e uma interface texto local.

- A interface gráfica

  A interface gráfica é chamada de remota porque através dela é possível se administrar remotamente, via Internet, um Firewall Aker localizado em qualquer parte do mundo. Esta administração é feita através de um canal seguro entre a interface e o firewall, com um forte esquema de autenticação e criptografia, de modo a torná-la totalmente segura.

A interface gráfica é de uso bastante intuitivo e esta disponível para plataformas Windows 95™, Windows 98™, Windows NT™, Windows 2000™ , Windows XP™ , Linux , FreeBSD e sob demanda em outros sabores de Unixes.

- A interface texto

A interface texto é uma interface totalmente orientada à linha de comando que roda na máquina onde o firewall está instalado. O seu objetivo básico é possibilitar a automação de tarefas da administração do Firewall Aker (através da criação de *scripts*) e possibilitar uma interação de qualquer *script* escrito pelo administrador com o Firewall.

Praticamente todas as variáveis que podem ser configuradas pela interface gráfica poderão ser configuradas também pela interface texto.

Como as duas interfaces tratam das mesmas variáveis, a funcionalidade, os valores e os comentários destas têm validade tanto para interface gráfica quanto para a interface texto. Devido a isso, os tópicos referentes à interface texto normalmente serão curtos e se limitarão a mostrar seu funcionamento. Caso se tenha dúvida sobre algum parâmetro, deve-se recorrer à explicação do mesmo no tópico relativo à interface gráfica.

Não é possível o uso simultâneo de várias interfaces gráficas para um mesmo Firewall, nem o uso da interface texto enquanto existir uma interface gráfica aberta.

Copyrights do Sistema

- Copyright (c) 1997-2003 Aker Security Solutions.
- utiliza a biblioteca SSL escrita por Eric Young (cay@mincon.oz.au). Copyright © 1995 Eric Young.
- utiliza o algoritmo AES implementação do Dr. B. R. Gladman (brg@gladman.uk.net).
- utiliza o algoritmo MD5 retirado da RFC 1321. Copyright © 1991-2 RSA Data Security, Inc.
- utiliza a biblioteca CMU SNMP. Copyright© 1997 Carnegie Mellon University.
- utiliza a biblioteca de compressão Zlib. Copyright © 1995-1998 Jean-loup Gailly and Mark Adler.
- utiliza a biblioteca QWT escrita por Josef Wilgen. Copyright © 1997.
- inclui software desenvolvido pela Universidade da California, Berkeley e seus colaboradores.
- inclui software desenvolvido por Luigi Rizzo, Universita` di Pisa Portions Copyright 2000 Akamba Corp.
- inclui software desenvolvido por Niklas Hallqvist, Angelos D. Keromytis and Haan Olsson.
- inclui software desenvolvido por Ericsson Radio Systems.

1-0 Instalando o Firewall Aker

Mostraremos neste capítulo todos os passos e requisitos necessários para se instalar o Firewall Aker.

1-1 Requisitos de hardware e software

Para o firewall

O Firewall Aker 5.1 roda sobre os sistemas operacionais Linux Red Hat 7.3, RedHat 9 e FreeBSD versões 4.9 e 4.11, em plataformas Intel ou compatíveis. Devido ao fato de quanto o Linux quanto o FreeBSD serem sistemas gratuitos, eles são distribuídos juntamente com a mídia de instalação do Firewall Aker. Desta forma, todo o software necessário para rodar o firewall já vem incluído com o mesmo. Não é necessária a compra de nenhum outro software adicional.

Quanto ao hardware, para que o Firewall Aker execute de maneira satisfatória, é necessária a seguinte lista (todos os componentes do hardware devem ser suportados pelo FreeBSD ou pelo Linux, em alguma das versões suportadas pelo firewall):

- Computador Pentium ou compatível 200 Mhz ou superior

Caso se utilize um link com alta taxa de transferência ou caso se pretenda utilizar criptografia em um link com velocidade relativamente alta é necessário o uso de um computador mais potente.

- 128 Mbytes de memória RAM

Caso se pretenda fazer um grande uso dos serviços de proxy e de criptografia, provavelmente será necessário 256 Mbytes ou mais.

- 4 Gbytes de espaço em disco

Pode ser necessário o uso de um disco maior caso se pretenda armazenar os logs do sistema por um grande espaço de tempo.

- Leitor de CD-ROM, monitor, mouse e teclado

Isso só é necessário durante a instalação ou caso se pretenda utilizar a interface texto a partir do console, entretanto é altamente recomendado em todos os casos.

- Placa(s) de rede

Não existe um número máximo de placas de rede que podem ser colocadas no Firewall. A única limitação existente é a limitação do próprio hardware. Caso se necessite de um grande número de interfaces de rede, pode-se optar por placas com mais de uma saída na mesma interface.

É importante frisar que todos os dispositivos de hardware devem ser suportados pelo FreeBSD ou pelo Linux. Antes de adquirir qualquer componente, é necessário primeiro se verificar se um destes sistemas operacionais, nas versões suportadas pelo Firewall Aker, aceita este componente.

Para maiores informações sobre os sistemas operacionais Linux ou FreeBSD ou para se verificar se um componente é ou não suportado por eles, sugerimos um dos seguintes endereços:

- WWW

http://www.br.freebsd.org (FreeBSD - português)
http://www.freebsd.org (FreeBSD - inglês)
http://www.linux.org (Linux - inglês)
http://www.kernel.org (Linux - inglês)
http://www.redhat.com (Linux - inglês)
http://www.conectiva.com.br (Linux - português)

- E-Mail

freebsd@sbq.org.br (lista de discussão de FreeBSD em português)
questions@freebsd.org (lista de discussão de FreeBSD em inglês)
linux-br-subscribe@bazar.conectiva.com.br (lista de discussão do Linux)

A Aker Security Solutions não se responsabiliza por nenhum problema de configuração, operação, compatibilidade ou informação relativa aos sistemas operacionais Linux ou FreeBSD.

Para a interface gráfica

A interface gráfica de adminstração do Firewall Aker roda em plataformas Windows 95 ou superiores, Linux Red Hat 7.3, 8 e 9 e Conectiva 8 e 9; FreeBSD versões 4.7 e 4.9, em plataformas Intel ou compatíveis.

Quanto ao hardware, para que a interace gráfica execute de maneira satisfatória, é necessária a seguinte lista (todos os componentes do hardware devem ser suportados pelo sistema operacional na qual a interface será instalada, em alguma das versões suportadas pelo produto):

- Computador Pentium II ou compatível 450 Mhz ou superior
- 128 Mbytes de memória RAM
- 4 Gbytes de espaço em disco
- Monitor
- Mouse
- Teclado
- Placa de rede

Para o servidor de log remoto

O servidor de log remoto do Firewall Aker roda em plataformas Windows NT ou superiores, Linux nas distribuições Red Hat 7.3, 8 e 9 e Conectiva 8 e 9; FreeBSD versões 4.7 e 4.9, em plataformas Intel ou compatíveis.

Quanto ao hardware, para que o servidor de log execute de maneira satisfatória, é necessária a seguinte lista (todos os componentes do hardware devem ser suportados pelo sistema operacional na qual o servidor será instalado, em alguma das versões suportadas pelo produto):

- Computador Pentium III ou compatível 1 Ghz ou superior
- Sistema de armazenagem com velocidade igual ou superior a um Ultra-ATA 66
- 64 Mbytes de memória RAM (recomenda-se 128 Mbytes)
- 40 Gbytes de espaço em disco
- Monitor
- Mouse
- Teclado
- Placa(s) de rede

1-2 Instalando o firewall

O Firewall Aker pode ser adquirido na forma de appliance. Sendo comprado desta forma, o produto já vem instalado e pré-configurado. Caso se tenha optado por comprar apenas o software, é necessário instalá-lo na máquina escolhida, o que será explicado neste tópico.

Para instalar o Firewall Aker, é necessário primeiro se instalar o sistema operacional Linux ou FreeBSD. A instalação de ambos é simples, porém recomenda-se que ela seja feita por alguém que possua algum conhecimento do sistema operacional Unix. O procedimento básico de instalação do FreeBSD e do Linux se encontra no seus CD-ROMs. Caso surjam problemas, sugerimos recorrer às fontes de informação mostradas no tópico anterior.

Após instalado o FreeBSD ou o Linux deve-se proceder com a instalação do Firewall Aker. Para instalá-lo, é necessário montar o CD-ROM de instalação na máquina que se deseja instalar ou copiar o conteúdo do diretório de instalação do CD-ROM para algum diretório temporário na máquina que se deseja instalar o produto (é possível se realizar esta cópia via FTP ou NFS, caso não se possua um leitor de CD-ROM na máquina na qual o produto deve ser instalado).

Após se realizar a montagem do CD-ROM, ou a cópia dos arquivos para um diretório qualquer, deve-se executar o seguinte comando:

#*/diretorio_de_instalacao*/br/firewall/*plataforma*/fwinst

Onde *diretório_de_instalação* é o diretório onde se encontram os arquivos de instalação e *plataforma* é a plataforma na qual o firewall será instalado, por exemplo, se o CD-ROM estivesse montando no diretório `/cdrom` e a instalação fosse feita no FreeBSD, então o comando a ser digitado seria: `/cdrom/br/firewall/freebsd/fwinst`

O símbolo # representa o prompt do shell quando executado como root, ele não deve ser digitado como parte do comando.

Instalando o Firewall no sistema operacional FreeBSD

O programa **fwinst** é o responsável por efetuar a instalação e a configuração do sistema para a execução do Firewall Aker. Ao ser executado, ele mostrará a seguinte tela:

```
                Firewall Aker v5.1 - Programa de Instalacao

Este programa realiza a instalacao do Firewall Aker 5 e da interface
texto de configuracao local.

A instalacao pode ser feita a partir de um kernel pre-compilado
fornecido
junto com o firewall, pode-se compilar um kernel especifico para esta
maquina
ou se utilizar o kernel atual (contanto que a versao 5 ou superior ja
tenha sido instalada anteriormente). O kernel pre-compilado possui
suporte
para 3 placas de rede isa e um numero ilimitado de placas de rede PCI.
Para
maiores informacoes, sobre quais placas sao suportadas, quais suas
configuracoes de endereco de E/S e IRQ e como alterar estes valores,
veja a
documentacao que acompanha o produto.

Caso se resolva compilar um kernel especifico, antes de executar este
programa
e' necessario a criacao de um arquivo de configuracao do kernel
chamado de
FIREWALL. Este arquivo deve estar localizado no diretorio
/usr/src/sys/i386/conf.

Deseja prosseguir com a instalacao do firewall (S/N) ?
```

Caso já se tenha criado o arquivo de configuração do kernel chamado de FIREWALL ou se deseje utilizar o kernel pré-compilado ou o atual , deve-se responder **S**, seguido de **Enter**, para continuar com a instalação. Caso se queira compilar um novo kernel e este arquivo ainda não tenha sido criado, deve-se digitar **N** e criá-lo, antes de se continuar.

Em caso de compilação de um novo kernel, existe um arquivo chamado de `FIREWALL`, no diretório de instalação, que pode ser utilizado como base para se gerar o arquivo customizado, apenas copiando-o para o diretório `/usr/src/sys/i386/conf` e removendo ou adicionando os componentes desejados. Para maiores informações sobre este arquivo, consulte a documentação do FreeBSD.

Caso se tenha feito a instalação do Firewall Aker com o kernel pré-compilado, ele estará configurado com suporte para até 10 (dez) VLANs, através do protocolo 802.1q .

A configuração das VLANs pode ser feita posteriormente utilizando-se a interface gráfica. Para mais informações leia a seção intitulada Configuração TCP/IP

Após se responder Sim, o programa de instalação mostrará a licença de uso do Firewall Aker. Para se prosseguir, é necessário aceitar todos os termos e condições contidas na licença. Caso sejam aceitos, o programa prosseguirá com a instalação mostrando a seguinte tela:

```
Firewall Aker v5.1 - Programa de Instalacao

Iniciando a instalacao:

Voce deseja utilizar o kernel (P)re-compilado, (C)ompilar um novo
kernel ou
usar o kernel (A)tual para a instalacao do firewall ? (P/C/A)
```

Caso se deseje utilizar o kernel pré-compilado, basta se digitar **P**, seguido de **Enter**. Caso se deseje utilizar o kernel atual, digita-se **A**. Caso contrário, digita-se **C**.

Recomenda-se a utilização do kernel pré-compilado, principalmente caso não se possua experiência prévia com o FreeBSD. A única necessidade de se compilar um novo kernel é para se utilizar uma versão mais otimizada do mesmo.

Só é possível se utilizar o kernel atual caso já se tenha instalado o Firewall Aker versão 5.1 na máquina anterioremente. Caso contrário deve-se escolher uma das duas outras opções.

Independente da opção escolhida, o programa iniciará a instalação propriamente dita. Ele mostrará o seu progresso através de uma série de mensagens auto-explicativas.

Deve-se atentar para o fato do programa de instalação substituir o arquivo **`/etc/rc`**. Caso se tenha feito alguma alteração neste arquivo é necessário fazê-la novamente após a instalação.

Após terminar de copiar os arquivos, o programa de instalação fará algumas perguntas de modo a realizar a configuração específica para cada sistema. A primeira destas configurações será a da chave de ativação do produto. Esta chave é o que habilita o produto para seu funcionamento. Sem ela nenhum módulo do firewall funcionará.

Será mostrada a seguinte tela:

```
Firewall Aker v5.1 - Programa de Instalacao
```

```
Configuracao do sistema completada. E' necessario agora ativar a copia
Instalada atraves da digitacao da chave de ativacao que foi entregue
ao
se adquirir o produto.

A chave de ativacao, o nome da empresa e o endereco IP da interface
externa deverao ser digitados exatamente como constam no documento
entregue pela Aker Consultoria e Informatica ou seu representante.

Pressione enter para continuar
```

Após digitar enter, o programa mostrará uma tela solicitando que se digite as informações contidas no documento fornecido pela Aker Security Solutions ou pelo seu representante autorizado de vendas. Deve-se atentar para digitar todos os campos exatamente como constam no documento.

A chave deve ser digitada com os hífens '-' que aparecem no documento original. No nome da empresa, letras maiúsculas e minúsculas são consideradas diferentes e devem ser digitadas exatamente como se encontram no documento original.

Um exemplo da entrada dos dados se encontra na tela mostrada abaixo:

```
                    Firewall Aker versao 5.1
              Modulo de configuracao da chave de ativacao

Nome da empresa: Aker Security Solutions
IP da interface externa: 10.0.0.1
Chave de ativacao: 2DBDC612-FA4519AA-BBCD0FF1-129768D3-89BCA59C
```

Caso a chave seja válida, o programa prosseguirá com a instalação. Caso a chave ou o nome da empresa tenham sido digitados com erro, o programa pedirá que sejam novamente digitados.

O endereço IP digitado deve ter sido previamente configurado em alguma interface do sistema, caso contrário o programa não prosseguirá com a instalação.

Caso a chave tenha sido aceita, a instalação prosseguirá. Neste ponto, o programa de instalação procurará por arquivos de configuração da versão 5.0 do Firewall Aker. Caso seja encontrado algum destes arquivos, a seguinte tela será mostrada:

```
                Firewall Aker v5.1 - Programa de Instalacao

Atualizando arquivos da versao 5.0 do Firewall Aker...
```

```
Atualizando mensagens e parametros... OK
Atualizando regras de filtragem... OK
Atualizando perfis de acesso... OK
Atualizando parametros de autenticacao... OK
Atualizando configuracoes do controle de acesso... OK
Atualizando parametros HTTP... OK
Atualizando configuracoes do balanceamento de links... OK
Atualizando configuracoes do controle de acesso por ip... OK

Atualizacao completa. Os arquivos de configuracao da versao 5.0 foram
removidos do sistema.

Pressione enter para continuar
```

A atualização dos arquivos é feita automaticamente e de forma a manter toda a configuração existente inalterada. Após realizada, os arquivos de configuração originais serão removidos do sistema e a seguinte tela será mostrada:

```
                Firewall Aker v5.1 - Programa de Instalacao

Criando servicos e regras padrao... OK

Voce deseja permitir que o firewall envie e receba 'pings', assim como
permitir que esses pacotes o atravessem para executar testes iniciais
de
conectividade (S/N)?
```

Caso se responda não à esta pergunta, o firewall será instalado através de uma política deny-all, ou seja, bloqueia todo o tráfego de rede, exceto o necessário para a administração remota. Após respondida esta pergunta, uma nova tela será mostrada:

```
                Firewall Aker v5.1 - Programa de Instalacao

E' necessario se definir o nome da interface de rede externa do
firewall
Os enderecos IP que se originarem desta interface nao serao
contabilizados
no numero maximo de licencas do produto.

A interface externa deve assumir um dos seguintes valores:

fxp0
fxp1
de0

Entre a interface externa:
```

A configuração da interface externa é usada apenas para o controle de licenças do firewall. Deve-se informar o nome da interface que estará conectada à Internet.

A especificação da interface externa não possui nenhuma implicação de segurança. Nenhum controle de acesso é feito levando-se em conta esta interface.

```
                Firewall Aker v5.1 - Programa de Instalacao

Ativacao do sistema completada. Vamos agora para a configuracao de
alguns
parametros do Firewall Aker:

Eu posso cadastrar automaticamente um administrador capaz
de gerenciar remotamente o firewall. Este administrador tera plenos
poderes em relacao
firewall e a partir dele novos usuarios poderao ser cadastrados.

Obs: Se voce nao cadastrar um administrador nao podera administrar o
firewall a partir da interface grafica, apenas atraves da interface
texto
local.

Voce deseja criar este administrador (S/N) ?
```

Para que seja possível se administrar o firewall a partir da interface gráfica, é necessário se cadastrar um administrador, devendo-se responder **S** a esta pergunta.

De qualquer forma, é possível se cadastrar posteriormente outros administradores através das interfaces locais de administração. A explicação de como fazer isso, se encontra no capítulo intitulado Administrando usuários do firewall.

Caso se tenha optado por incluir um novo administrador, será mostrada a tela pedindo os dados do administrador a ser cadastrado. Um exemplo desta tela se encontra abaixo (cabe mencionar que a senha do administrador a ser cadastrado não será mostrada na tela).

```
                        Firewall Aker versao 5
                Modulo de administracao de usuarios remotos
                          Inclusao de usuario

Entre o login         : administrador
Entre o nome completo : Administrador do Firewall Aker
Entre a senha         :
Confirme a senha      :


                Confirma inclusao do usuario ? (S/N)
```

Após se ter ou não incluído o administrador, será mostrada uma mensagem perguntando sobre o cadastro de um segredo compartilhado para administração do Firewall através do Aker Configuration Manager. Se você não tem este produto, responda **não**, caso contrário consulte o manual do mesmo.

Caso se tenha definido que se irá compilar um novo kernel, o programa de instalação mostrará uma última tela informando que ele iniciará a compilação de um novo kernel para a máquina, com base no arquivo de configuração do kernel chamado **/usr/src/sys/i386/conf/FIREWALL.**

```
                Firewall Aker v5.1 - Programa de Instalacao

Irei agora realizar a compilacao do kernel para instalar o Firewall
Aker
nesta maquina. Esta compilacao pode levar de 5 a 40 minutos,
dependendo
sua configuracao e da velocidade de sua maquina.

Pressione enter para continuar
```

Ao se pressionar enter, o programa iniciará a compilação do novo kernel. Após compilar e instalar o novo kernel, ele solicitará que a máquina seja reinicializada para ativar o Firewall Aker. Ao se reinicializar a máquina, o firewall já entrará em funcionamento automaticamente e poderá ser configurado remotamente.

Instalando o Firewall no sistema operacional Linux

O programa **fwinst** é o responsável por efetuar a instalação e a configuração do sistema para a execução do Firewall Aker. Ao ser executado, ele mostrará a seguinte tela:

```
                Firewall Aker v5.1 - Programa de Instalacao

Este programa realiza a instalacao do Firewall Aker 5 e da interface
texto de configuracao local.

O Firewall Aker 5 pode ser instalado no kernel distribuido junto com o
Linux
Red Hat 7.3 ou Conectiva 8 e 9. Desta forma, nao e' necessario
recompila-lo.

Deseja prosseguir com a instalacao do firewall (S/N) ?
```

Após se responder Sim, o programa de instalação mostrará a licença de uso do Firewall Aker. Para se prosseguir, é necessário aceitar todos os termos e condições contidas na licença. Caso sejam aceitos, o programa prosseguirá com a instalação mostrando seu progresso através de uma série de mensagens auto-explicativas.

Após terminar de copiar os arquivos, o programa de instalação fará algumas perguntas de modo a realizar a configuração específica para cada sistema. A primeira destas configurações será a da chave de ativação do produto. Esta chave é o que habilita o produto para seu funcionamento. Sem ela nenhum módulo do firewall funcionará.

Será mostrada a seguinte tela:

```
                Firewall Aker v5.1 - Programa de Instalacao

Configuracao do sistema completada. E' necessario agora ativar a copia
Instalada atraves da digitacao da chave de ativacao que foi entregue
ao
se adquirir o produto.

A chave de ativacao, o nome da empresa e o endereco IP da interface
externa deverao ser digitados exatamente como constam no documento
entregue pela Aker Consultoria e Informatica ou seu representante.

Pressione enter para continuar
```

Após digitar enter, o programa mostrará uma tela solicitando que se digite as informações contidas no documento fornecido pela Aker Security Solutions ou pelo seu representante autorizado de vendas. Deve-se atentar para digitar todos os campos exatamente como constam no documento.

A chave deve ser digitada com os hífens '-' que aparecem no documento original. No nome da empresa, letras maiúsculas e minúsculas são consideradas diferentes e devem ser digitadas exatamente como se encontram no documento original.

Um exemplo da entrada dos dados se encontra na tela mostrada abaixo:

```
                    Firewall Aker versao 5
              Modulo de configuracao da chave de ativacao

Nome da empresa: Aker Security Solutions
IP da interface externa: 10.0.0.1
Chave de ativacao: 2DBDC612-FA4519AA-BBCD0FF1-129768D3-89BCA59C
```

Caso a chave seja válida, o programa prosseguirá com a instalação. Caso a chave ou o nome da empresa tenham sido digitados com erro, o programa pedirá que sejam novamente digitados.

O endereço IP digitado deve ter sido previamente configurado em alguma interface do sistema, caso contrário o programa não prosseguirá com a instalação.

Caso a chave tenha sido aceita, a instalação prosseguirá. Neste ponto, o programa de instalação procurará por arquivos de configuração da versão 5.0 do Firewall Aker. Caso seja encontrado algum destes arquivos, a seguinte tela será mostrada:

```
                Firewall Aker v5.1 - Programa de Instalacao

Atualizando arquivos da versao 5.0 do Firewall Aker...

Atualizando mensagens e parametros... OK
Atualizando regras de filtragem... OK
Atualizando perfis de acesso... OK
Atualizando parametros de autenticacao... OK
Atualizando configuracoes do controle de acesso... OK
Atualizando parametros HTTP... OK
Atualizando configuracoes do balanceamento de links... OK
Atualizando configuracoes do controle de acesso por ip... OK

Atualizacao completa. Os arquivos de configuracao da versao 5.0 foram
removidos do sistema.

Pressione enter para continuar
```

A atualização dos arquivos é feita automaticamente e de forma a manter toda a configuração existente inalterada. Após realizada, os arquivos de configuração originais serão removidos do sistema e a seguinte tela será mostrada:

```
                Firewall Aker v5.1 - Programa de Instalacao

Criando servicos e regras padrao... OK

Voce deseja permitir que o firewall envie e receba 'pings', assim como
permitir que esses pacotes o atravessem para executar testes iniciais
de
conectividade (S/N)?
```

Caso se responda não à esta pergunta, o firewall será instalado através de uma política deny-all, ou seja, bloqueia todo o tráfego de rede, exceto o necessário para a administração remota. Após respondida esta pergunta, uma nova tela será mostrada:

```
                Firewall Aker v5.1 - Programa de Instalacao

E' necessario se definir o nome da interface de rede externa do
firewall
Os enderecos IP que se originarem desta interface nao serao
contabilizados
no numero maximo de licencas do produto.

A interface externa deve assumir um dos seguintes valores:

eth0
eth1
eth2

Entre a interface externa:
```

A configuração da interface externa é usada apenas para o controle de licenças do firewall. Deve-se informar o nome da interface que estará conectada à Internet.

A especificação da interface externa não possui nenhuma implicação de segurança. Nenhum controle de acesso é feito levando-se em conta esta interface.

```
                Firewall Aker v5.1 - Programa de Instalacao

Ativacao do sistema completada. Vamos agora para a configuracao de
alguns
parametros do Firewall Aker:

Eu posso cadastrar automaticamente um administrador capaz de gerenciar
remotamente o firewall. Este administrador tera plenos poderes em
relacao
firewall e a partir dele novos usuarios poderao ser cadastrados.

Obs: Se voce nao cadastrar um administrador nao podera administrar o
firewall a partir da interface grafica, apenas atraves da interface
texto
local.

Voce deseja criar este administrador (S/N) ?
```

Para que seja possível se administrar o firewall a partir da interface gráfica, é necessário se cadastrar um administrador, devendo-se responder **S** a esta pergunta.

De qualquer forma, é possível se cadastrar posteriormente outros administradores através das interfaces locais de administração. A explicação de como fazer isso, se encontra no capítulo intitulado Administrando usuários do firewall.

Caso se tenha optado por incluir um novo administrador, será mostrada a tela pedindo os dados do administrador a ser cadastrado. Um exemplo desta tela se encontra abaixo (cabe mencionar que a senha do administrador a ser cadastrado não será mostrada na tela).

```
                    Firewall Aker versao 5.1
            Modulo de administracao de usuarios remotos
                      Inclusao de usuario

Entre o login         : administrador
Entre o nome completo : Administrador do Firewall Aker
Entre a senha         :
Confirme a senha      :

                Confirma inclusao do usuario ? (S/N)
```

Após se ter ou não incluído o administrador, será mostrada uma mensagem perguntando sobre o cadastro de um segredo compartilhado para administração do Firewall através do Aker Configuration Manager. Se você não tem este produto, responda **não**, caso contrário consulte o manual do mesmo.

Finalmente, será mostrada uma mensagem indicando o término da instalação e solicitando que a máquina seja reinicializada para ativar o Firewall Aker. Ao se reinicializar a máquina, o firewall já entrará em funcionamento automaticamente e poderá ser configurado remotamente.

1-3 Instalando a interface remota

Em plataformas Windows

Para instalar a interface remota nas plataformas Windows 95, 98, Me, NT, 2000 ou XP, deve-se colocar o CD-ROM do Aker Security Suite no drive e seguir as instruções que aparecerão na tela.

Caso a opção de auto-execução esteja desabilitada, então é necessário se executar os seguintes passos:

1. Clicar no menu **Iniciar**
2. Selecionar a opção **Executar**
3. Ao ser perguntado sobre qual programa executar, digitar ***D:\br\control_center\AkerRemoteDesktop-br-win-5.1-1*** (Caso o leitor de CD-ROM seja acessado por uma letra diferente de **D**, substituí-la pela letra equivalente, no comando anterior).

Ao término da instalação, será criado um grupo chamado **Aker**, no menu **Iniciar**. Para executar a interface remota, basta selecionar a opção **Firewall 5 GUI** dentro deste grupo.

Em plataformas Linux

Para instalar a interface remota em plataformas Linux é necessário que os pacotes da biblioteca QT estejam previamente instalados.

A interface gráfica para plataformas Linux é distribuída em pacotes RPM. Para instalá-la, proceda da seguinte forma (exemplo para Red Hat 9):

1. Coloque o CD-ROM no drive e monte-o, através do comando **`mount /mnt/cdrom`**
2. Execute o comando: **`rpm -ivh /mnt/cdrom/br/control_center/rh9/aker_control_center-br-1.0-1.i386.rpm`**
3. Execute o comando: **`rpm -ivh /mnt/cdrom/br/control_center/rh9/fwgui-br-man-1.0-1.i386.rpm`**
4. Após a apresentação de cerquilhas a interface estará instalada.

Os nome do pacote a ser instalado pode mudar conforme a versão do Linux no qual a interface será instalada. Verifique o conteúdo do diretório **`/mnt/cdrom/br/control_center/`** para ver os nomes de todos os pacotes e selecionar o mais adequado.

Em plataformas FreeBSD

Para instalar a interface remota em plataformas FreeBSD é necessário que os pacotes da biblioteca QT estejam previamente instalados.

A interface gráfica para o FreeBSD será distribuída em pacotes tbz. Para instalar a interface neste sistema operacional proceda da seguinte forma:

1. Coloque o CD-ROM no drive e monte-o, através do comando **`mount /cdrom`**
2. Execute o comando: **`pkg_add /mnt/cdrom/br/remote_desktop/free/aker_control_center-br-1.0.tbz`**
3. Execute o comando: **`pkg_add /mnt/cdrom/br/remote_desktop/free/fwgui-br-man-5.1.tbz`**
4. Após o retorno do prompt de comando a interface estará instalada.

O nome do pacote a ser instalado pode mudar conforme a versão do FreeBSD no qual a interface será instalada. Verifique o conteúdo do diretório **`/cdrom/br/control_center/`** para ver os nomes de todos os pacotes e selecionar o mais adequado.

2-0 Utilizando a Interface Remota

Neste capítulo mostraremos como funciona a interface gráfica remota de administração do Firewall Aker.

O que é a administração remota do Firewall Aker ?

O Firewall Aker pode ser totalmente configurado e administrado remotamente, a partir de qualquer máquina que possua um sistema operacional compatível com uma das versões da interface remota, que tenha TCP/IP e que consiga acessar a máquina na qual o firewall se encontra. Isto permite um alto grau de flexibilidade e facilidade de administração, possibilitando que um administrador monitore e configure vários firewalls a partir de sua estação de trabalho.

Além dessa facilidade, a administração remota permite uma economia de recursos na medida em que possibilita que a máquina que rode o firewall não possua monitor e outros periféricos.

Como funciona a administração remota do Firewall Aker ?

Para possibilitar a administração remota, existe um processo rodando na máquina do firewall responsável por receber as conexões, validar os usuários e executar as tarefas solicitadas por estes usuários. Quando um usuário inicia uma sessão de administração remota, a interface gráfica estabelece uma conexão com o módulo de administração remota do firewall e mantém esta conexão aberta até que o usuário finalize a sessão.

Toda a comunicação entre a interface remota e o firewall é feita de maneira segura, utilizando-se criptografia e autenticação. Para cada sessão, são geradas novas chaves de criptografia e autenticação. Além disso, são empregadas técnicas de segurança para impedir outros tipos de ataques, como por exemplo, ataques de repetição de pacotes.

Existem algumas observações importantes sobre a administração remota que devem ser comentadas:

1. Para que a interface remota consiga se conectar ao firewall, é necessário a adição de uma regra liberando o acesso **TCP** para a porta **1020** a partir da máquina que deseja se conectar. Informações de como fazer isso se encontram no capítulo intitulado O Filtro de Estados.
2. Só é possível a abertura de uma conexão de administração remota em um determinado instante. Se já existir uma interface conectada, pedidos subseqüentes de conexão serão recusados e a interface remota informará que já existe uma sessão ativa.
3. Cada um dos usuários que for utilizar a interface remota deve estar cadastrado no sistema. O programa de instalação pode criar automaticamente um administrador com poderes para cadastrar os demais administradores. Caso se tenha eliminado este administrador ou perdido sua senha, é necessário o uso do módulo local da interface gráfica ou da interface texto para criar um novo

administrador. Detalhes de como fazer isso se encontram no capítulo intitulado Administrando Usuários do Firewall.

Como utilizar a interface

A interface é bastante simples de ser utilizada, entretanto, existe uma observação que deve ser comentada:

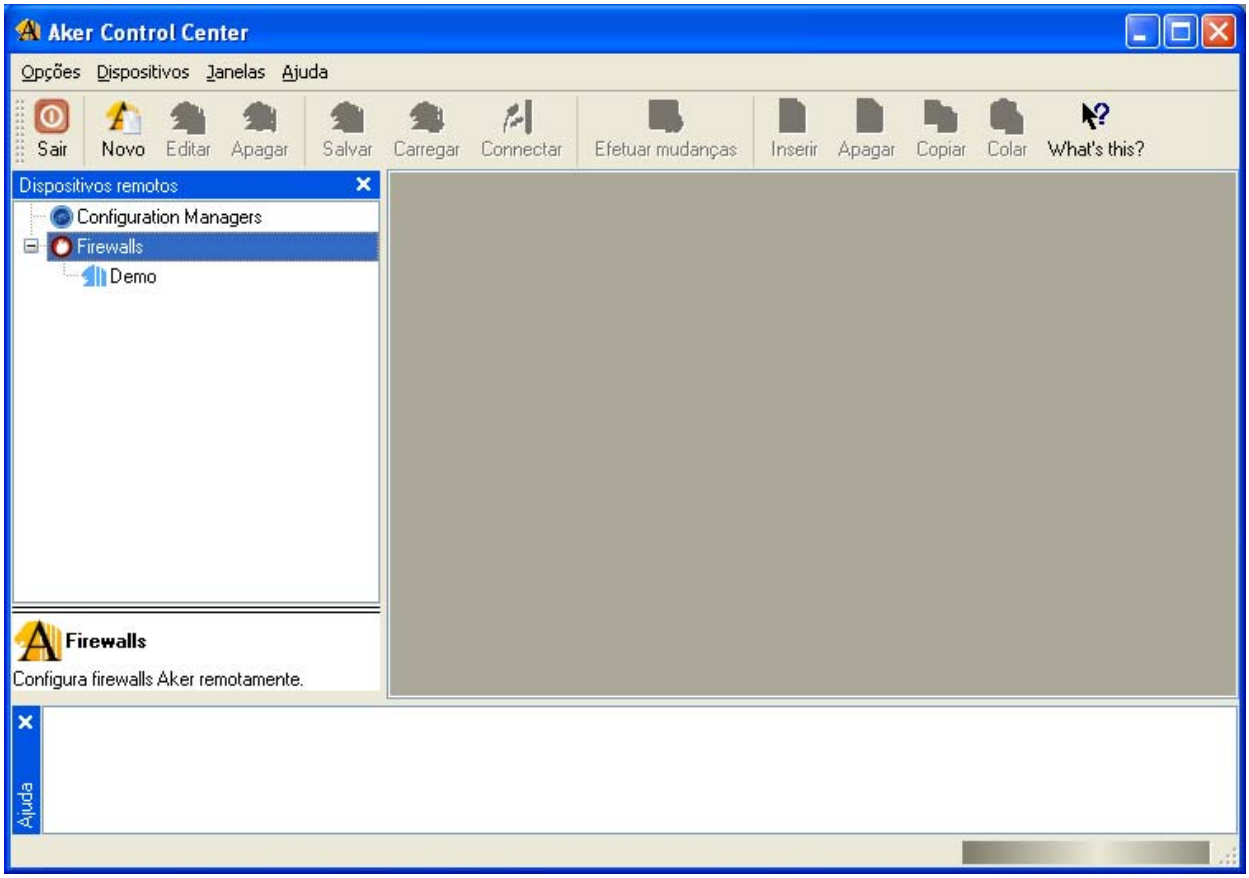
Os botões esquerdo e direito do mouse tem funções diferentes na interface. O botão esquerdo é usado para se selecionar entradas em uma lista e para se clicar em botões. O botão direito tem como função mostrar um menu de opções para uma determinada lista.

2-1 Iniciando a interface remota

Para iniciar a execução da interface gráfica remota deve-se executar um dos seguintes passos:

- Em máquinas Windows, clicar no menu **Iniciar**, selecionar o grupo **Aker**, dentro deste grupo selecionar o sub-grupo **Aker Control Center** e clicar no ícone **Aker Control Center.**
- Em FreeBSD ou Linux, deve-se executar o comando '`fwgui`' a partir do prompt do shell ou clicar no ícone criado na área de trabalho (apenas para KDE).

Será mostrada a seguinte janela:



A janela mostrada acima é a janela principal do Firewall Aker. É a partir dela que se tem acesso a todas as opções de configuração. Ela consiste de 4 menus, descritos brevemente abaixo (quando existe um firewall selecionado, um quinto menu é mostrado com opções específicas para o firewall selecionado):

- **Opções**

O menu *Opções* contém as configurações relacionadas ao layout da interface gráfica. Ao se clicar neste menu, aparecerão as seguintes opções:

- Textos nos botões: marcando esta opção será mostrada juntamente com cada ícone a ação correspondente do botão. Desmarcando esta opção, será mostrado apenas o ícone.

- Dicas para Entidades: quando esta opção estiver ativada uma pequena caixa com a descrição de cada entidade irá aparecer quando o mouse for passado sobre seu ícone, conforme a figura abaixo.

- Ajuda Rápida: esta opção ativa o help contextual automático para cada janela.

- Mostrar ícones nos botões: esta opção, se ativada, faz com que sejam mostrados ícones nos botões *Ok*, *Cancelar* e *Aplicar* das janelas.

- Tempo de sessão ociosa...<>: Permite definir o tempo máximo, em minutos, que a interface permanecerá conectada ao firewall sem receber nenhum comando do administrador. Assim que este tempo limite for atingido, a interface automaticamente se desconectará do firewall, permitindo que uma nova sessão seja estabelecida. Seu valor pode variar entre 1 e 60. A caixa "Sem limite" quando estiver marcada não desconectará a interface do firewall.
Valor padrão: **1** minuto.

- Sair: fecha a janela da interface gráfica.

- **Firewalls**

Este menu serve para se cadastrar mais firewalls na interface gráfica de modo a possibilitar a administração de diversos Firewalls Aker simultaneamente. Com a interface conectada a mais de um firewall simultaneamente, é possível se usar a facilidade de arrastar-e-soltar as entidades e regras entre firewalls, de modo a facilitar a replicação de determinadas configurações entre eles. Este menu será descrito em detalhes mais abaixo.

- **Janelas**

Este menu possui as funções de configuração das janela abertas e da barra de menu.

- Barra de ferramentas: esta opção permite que se defina se a barra de ferramentas na parte superior da janela principal será mostrada ou não.

- Janelas: esta opção permite que se mostre ou não as janelas padrão do sistema: *ajuda*, *firewalls* e *entidades*.

- Lado a Lado: selecionando esta opção, as janelas abertas do lado direito da interface gráfica se ajustam de forma que todas aparecem visíveis.

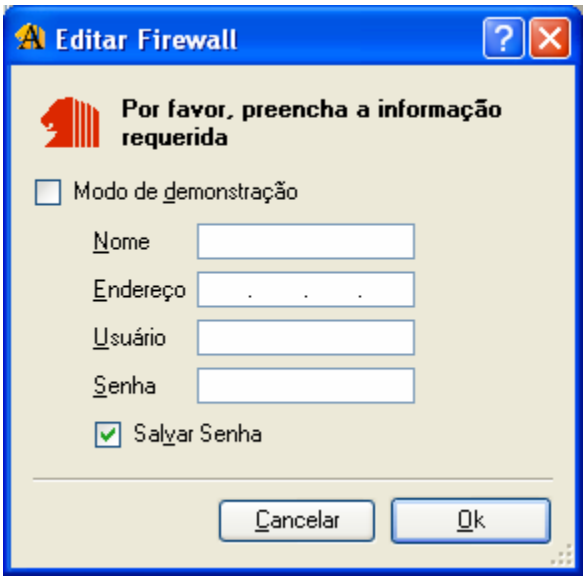
- Cascata: esta opção faz com que as janelas abertas no lado direito da interface gráfica fiquem posicionadas em forma de cascata, uma na frente da outra.

Inicialmente, nem todas as opções dos menus se encontram habilitadas, por funcionarem apenas quando houver uma conexão estabelecida. Para se ter acesso às demais opções é necessário que se estabeleça uma sessão de administração remota com o firewall que se deseja administrar. Para tanto deve-se seguir os seguintes passos:

- Cadastrar o firewall selecionando-se o menu *Firewalls* e a opção *Novo Firewall* (veja o item Cadastrando Firewalls logo a seguir)
- Selecionar o firewall com o qual se desejar conectar
- Clicar na opção *Conectar*

Cadastrando Firewalls

Nesta seção demonstraremos como podemos cadastrar um (ou mais) firewalls. Quando selecionamos a opção *Novo Firewall* dentro do menu *Firewalls* ou no ícone *"Criar novo Firewall"* aparecerá a seguinte janela:



- **Modo de demonstração**: caso esta opção for marcada, será criado um firewall de demonstração, com uma configuração padronizada. Nenhuma conexão real será feita ao

se tentar conectar neste firewall, podendo-se criar quantos firewall de demonstração for desejado, cada um com sua configuração distinta do outro;

- **Nome**: este campo é usado para se cadastrar o nome pelo qual o firewall será referenciado na interface gráfica;

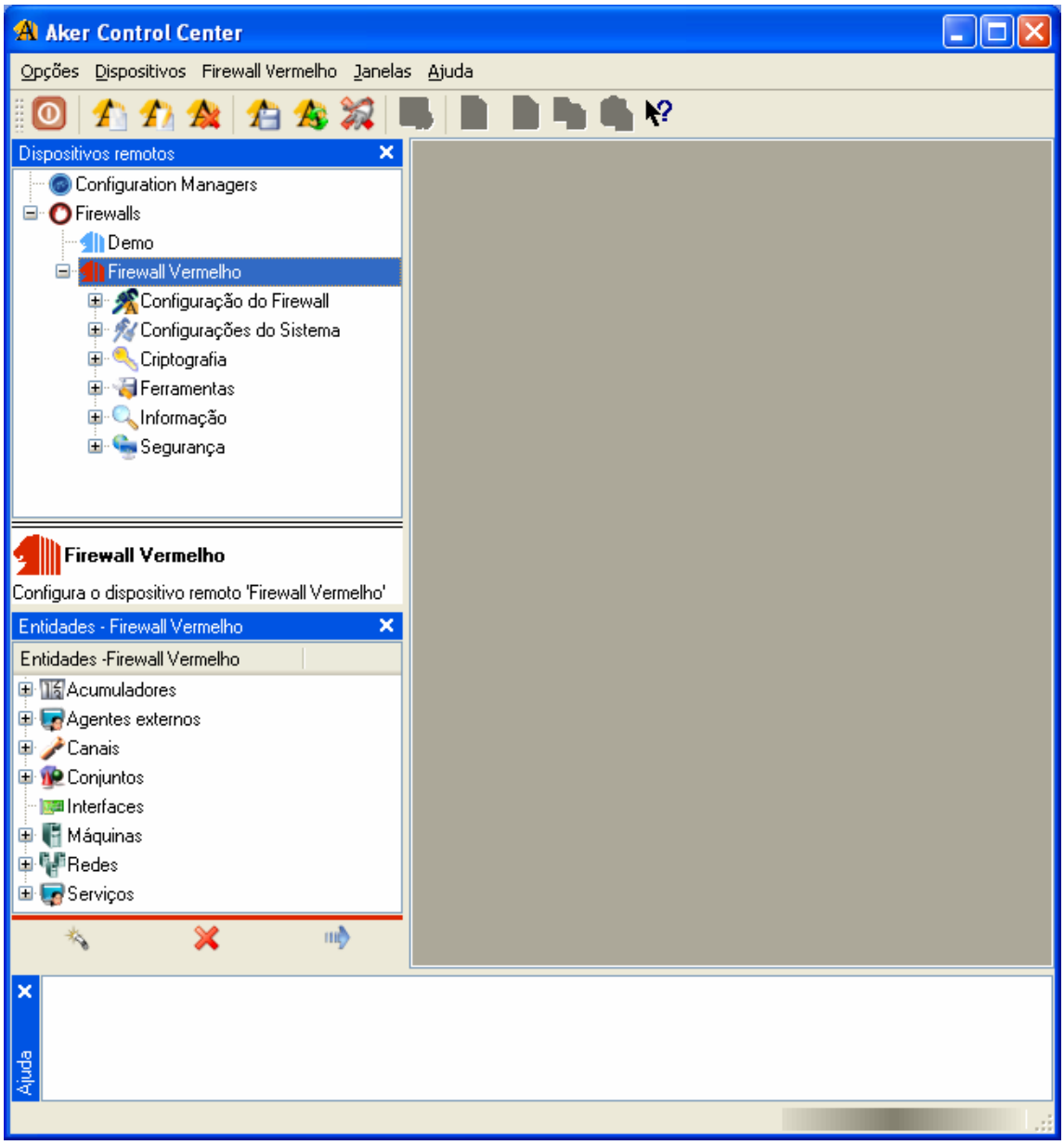
- **Endereço**: campo para cadastrar o endereço IP o qual nos conectaremos no firewall;

- **Usuário**: o usuário que acessará o firewall. Este campo serve para que não precisemos digitar o usuário quando quisermos acessar o firewall, já que ficará gravado.

- **Senha**: a senha do usuário. Caso deixe a caixa *Salvar senha* marcada, não será necessário digitar a senha quando fizer a conexão (a senha aparecerá na tela como vários asteriscos "*"). Caso ela esteja desmarcada, este campo estará desabilitado.

No final basta clicar em **Ok** e o firewall estará cadastrado. No caso de cancelar o cadastro do firewall, basta clicar em **Cancelar**.

Depois de cadastrarmos o firewall, podemos clicar duas vezes no ícone do firewall criado, no lado esquerdo da janela, ou clicar uma vez para selecioná-lo e, em seguida, no botão *Conectar* que fará com que a interface se conecte ao firewall escolhido, como mostrado na figura abaixo:



Caso não seja possível estabelecer a sessão de administração, será mostrada uma janela com o erro que impossibilitou sua abertura. Neste caso, existem várias mensagens possíveis. Abaixo estão listadas as mensagens de erro mais comuns:

- Aker já sendo utilizado por outra interface

O Firewall Aker só permite a existência de uma sessão de administração em um determinado instante. Se esta mensagem for mostrada, significa que já existe uma outra interface remota conectada ou um módulo de administração local sendo utilizado.

- Erro de rede ou conexão encerrada pelo servidor

Este é um erro genérico e pode ter uma série de causas. A sua causa mais comum é um erro na digitação do login ou da senha. Se o login do usuário não estiver cadastrado ou sua senha estiver errada, o servidor encerrará a conexão. Verifique primeiramente se seu

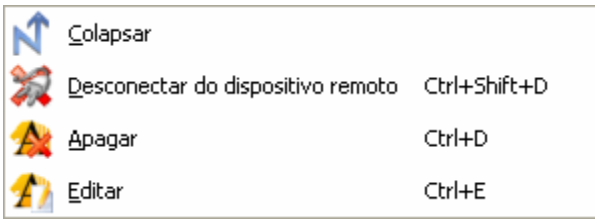
login e sua senha foram digitados corretamente. Caso o erro continue, siga a seguinte seqüência de passos:

1. Verifique se o usuário que está tentando se conectar está cadastrado no sistema e a sua senha está correta (para fazer isso, utilize o módulo local de administração de usuários. Veja o capítulo intitulado Administrando usuários do firewall).
2. Verifique se a rede está funcionando corretamente. É possível se fazer isso de várias formas, uma delas é utilizando o comando **ping**. (Não se esqueça de acrescentar uma regra liberando os serviços ICMP echo request e echo reply para a máquina que se está testando em direção ao firewall, caso se vá utilizar o ping. Para aprender como fazer isso, veja o capítulo intitulado O Filtro de Estados). Se isso não funcionar, então a rede está com problemas de conectividade e isto deve ser corrigido antes de se tentar a administração remota. Caso funcione, veja o passo 3.
3. Verifique se existe uma regra cadastrada liberando o acesso a partir da máquina que se deseja conectar para o firewall, utilizando o serviço Aker (TCP, porta 1020). Caso não exista, insira esta regra (para aprender como fazer isso, veja o capítulo intitulado O Filtro de Estados)

2-2 Finalizando a administração remota

Existem três formas de finalizar a administração remota do Firewall Aker:

- Finalizando a sessão clicando com o botão direito do mouse no firewall conectado e selecionando *Desconectar do dispositivo remoto*;



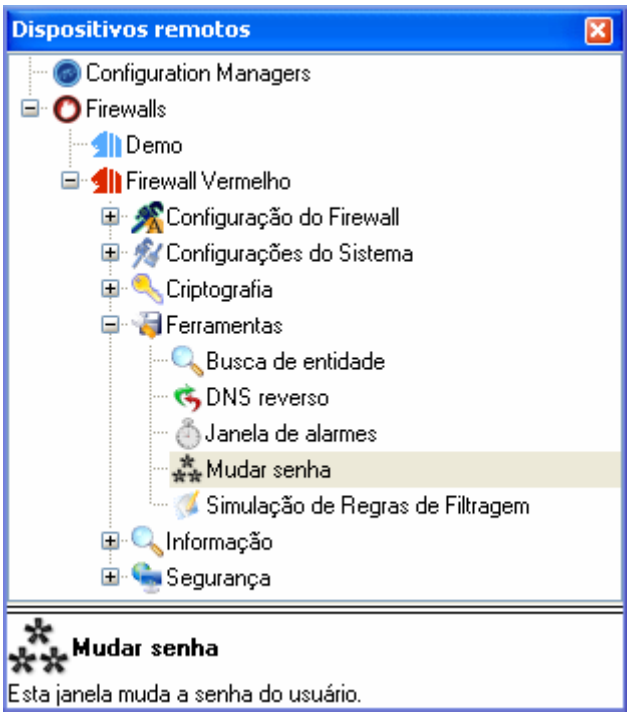
- Clicando em *Desconectar do firewall* na barra de ferramentas ou

- Fechando a interface gráfica remota. Neste caso você perderá a conexão com todos os firewalls que estiverem conectados.

Caso se deseje sair do programa, basta clicar no botão *Sair* na barra de ferramentas da janela principal ou clicar no "x" no canto superior direito da janela.

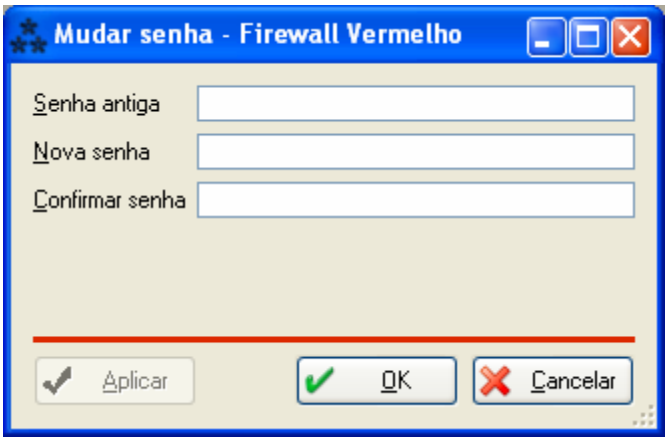
2-3 Mudando sua senha de usuário

É possível para qualquer usuário do Firewall Aker alterar a sua senha sempre que desejado. Para tanto deve-se primeiro estabelecer uma sessão de administração (como mostrado no tópico Iniciando a interface remota) e após isso executar os seguintes passos:



- Selecionar o firewall a ser configurado
- Clicar em *Ferramentas*
- Clicar duas vezes em *Mudar senha.*

Será mostrada então a seguinte janela:



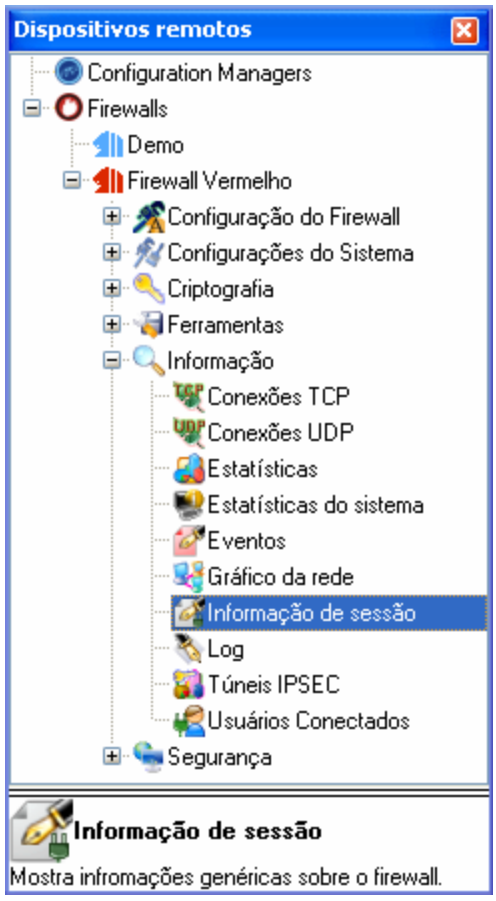
Deve-se digitar a senha anterior no campo **Senha antiga** e digitar a nova senha nos campos **Nova senha** e **Confirmar a nova senha** (as senhas aparecerão na tela como vários asteriscos "*").

Após preencher os campos, deve-se pressionar o botão **OK**, para alterar a senha ou o botão **Cancelar**, caso não se deseje mudá-la.

2-4 Visualizando informações da sessão

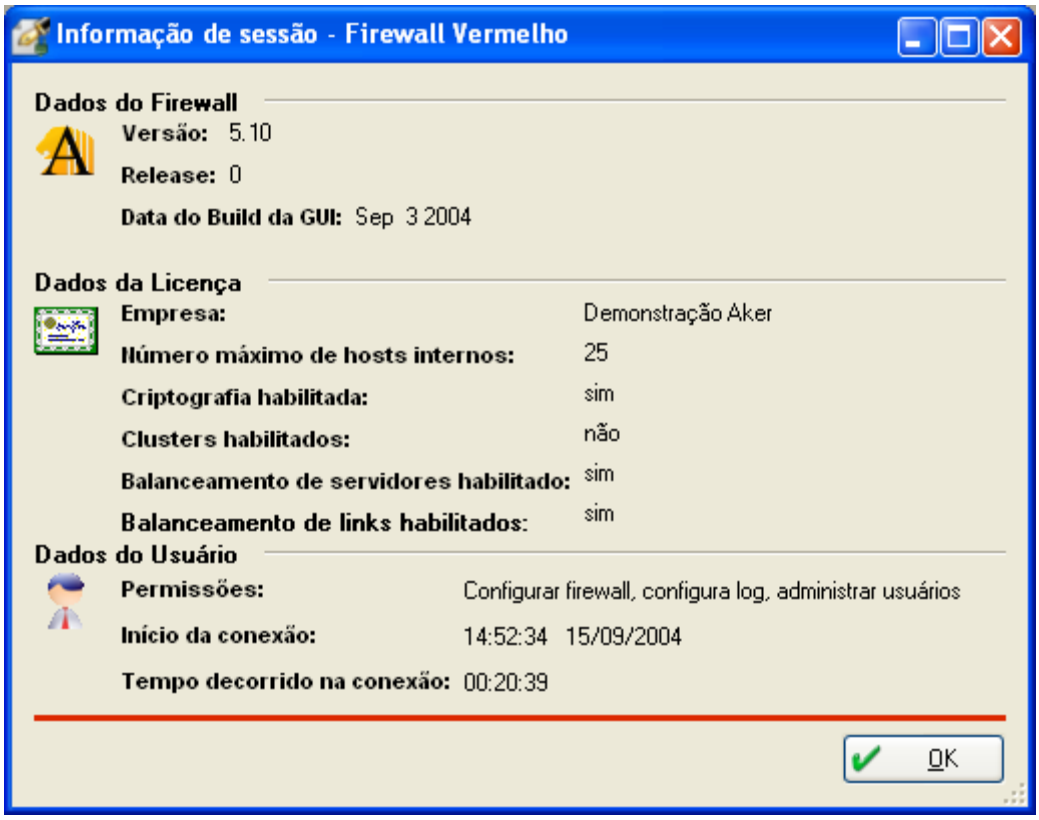
É possível a qualquer momento visualizar algumas informações sobre a sessão de administração ativa. Para isso existe uma janela específica que mostra informações úteis

como: login, nome e direitos do usuário que está administrando o firewall e a versão e o release do Firewall Aker que estiver sendo administrado. São mostradas também a hora de início da conexão e a quanto tempo ela está ativa. Para abrir esta janela, execute os seguintes passos:



- Selecionar o firewall a ser configurado
- Clicar em *Informação*
- Clicar duas vezes em *Informação de sessão.*

Será mostrada então a seguinte janela:

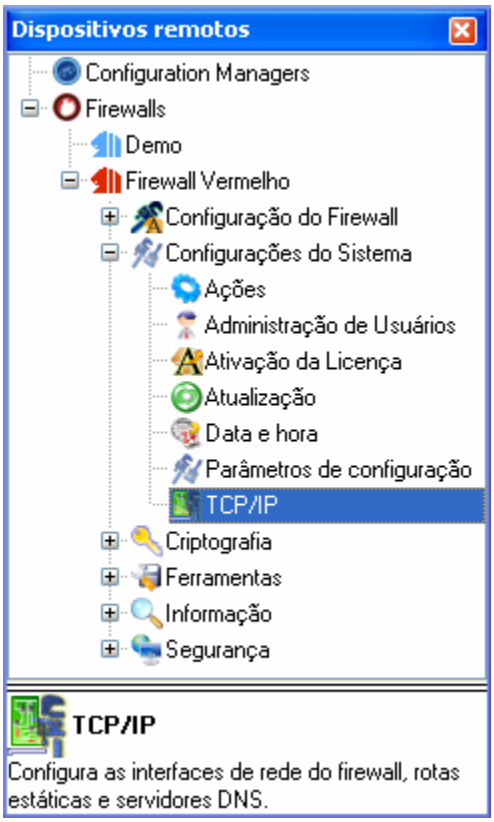

Informação de sessão - Firewall Vermelho
Dados do Firewall
Versão: 5.10
Release: 0
Data do Build da GUI: Sep 3 2004
Dados da Licença
Empresa: Demonstração Aker
Número máximo de hosts internos: 25
Criptografia habilitada: sim
Clusters habilitados: não
Balanceamento de servidores habilitado: sim
Balanceamento de links habilitados: sim
Dados do Usuário
Permissões: Configurar firewall, configura log, administrar usuários
Início da conexão: 14:52:34 15/09/2004
Tempo decorrido na conexão: 00:20:39
OK

2-5 Utilizando a ajuda on-line e a Ajuda-Rápida

O Firewall Aker possui uma ajuda on-line bastante completa. Ela é mostrada em uma janela ao final da interface gráfica. Esta janela pode ser escondida ou mostrada, sendo possível se escolher qual das duas formas através do menu *Janelas*, Sub-menu *Janelas*, opção *Ajuda*.

A ajuda on-line consiste do conteúdo deste manual mostrado de forma sensível ao contexto em relação à janela de configuração do firewall ativa, ou seja, será mostrada a parte do manual que seja relevante para a janela que se esteja configurando.

A Ajuda-Rápida consiste em uma breve explicação sobre cada um dos itens dos menus de configuração. Esta explicação é mostrada em uma pequena janela, abaixo dos menus, como destacado abaixo:



É possível mostrar ou esconder a Ajuda-Rápida, bastando clicar na opção *Ajuda Rápida* do menu *Opções*.

3-0 Administrando Usuários do Firewall

Neste capítulo mostraremos como criar os usuários que irão administrar remotamente o Firewall Aker.

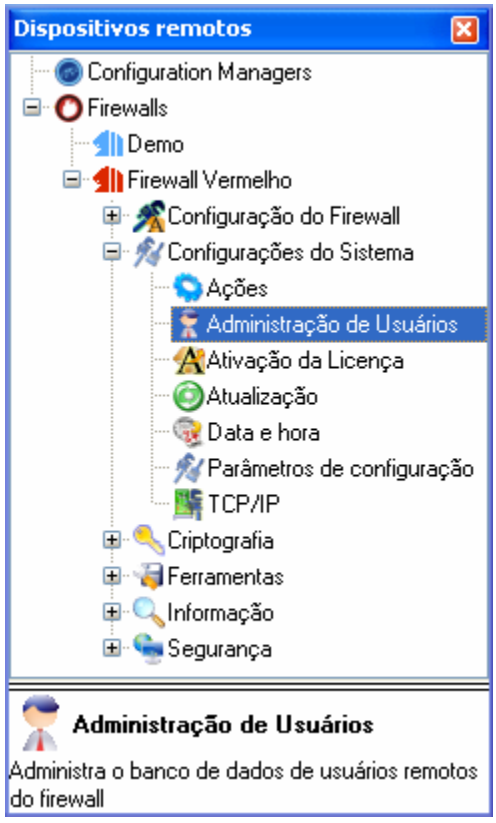
O que são usuários do Firewall Aker ?

Para que alguma pessoa consiga administrar remotamente o Firewall Aker, é necessário que esta seja reconhecida e validada pelo sistema. Esta validação é feita na forma de senhas e, para que ela seja possível, cada um dos administradores deverá ser previamente cadastrado com um login e uma senha.

Além disso, o Firewall Aker permite a existência de vários administradores distintos, cada um responsável por uma determinada tarefa da administração. Isto além de facilitar a administração, permite um maior controle e uma maior segurança. É no cadastro de usuários que se define as atribuições de cada um dos administradores.

3-1 Utilizando a interface gráfica

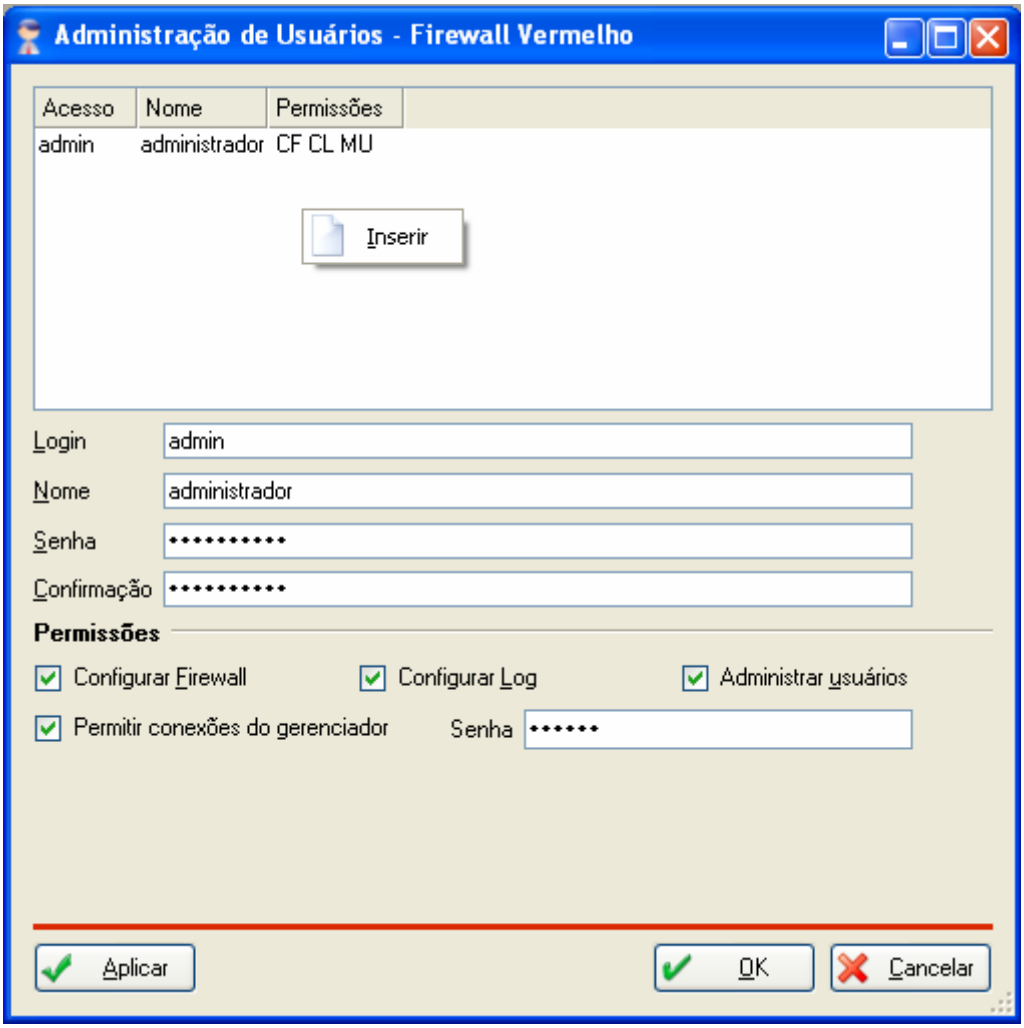
Para ter acesso a janela de administração de usuários na interface remota basta:



- Clicar em *Configurações do Sistema* da janela do firewall que se quer administrar
- Selecionar o item *Administração de Usuários*

Esta opção só estará habilitada se o usuário que estiver com a sessão aberta na interface remota tiver autoridade para gerenciar usuários. Isto será comentado em detalhes no próximo tópico.

A janela de administração de usuários



Esta janela consiste de uma lista de todos os usuários atualmente definidos para acesso à administração do firewall, além de um segredo compartilhado (ou senha), para administração centralizada pelo Aker Configuration Manager. Não havendo o segredo compartilhado, a configuração será apenas efetuado pelos usuários cadastrados.

Para cada usuário, é mostrado seu login, seu nome completo e suas permissões.

- O botão **OK** fará com que a janela de administração de usuários seja fechada e as modificações salvas.
- O botão **Aplicar** fará com que as alterações realizadas sobre um determinado usuário sejam aplicadas, isto é, realizadas permanentemente, sem fechar a janela.
- O botão **Cancelar** fechará a janela de administração de usuários e descartará todas as alterações efetuadas.

- Quando um usuário for selecionado, os seus atributos completos serão mostrados nos campos Permissões.

Para se alterar os atributos de um usuário, deve-se proceder da seguintes forma:

1. Seleciona-se o usuário a ser alterado clicando sobre seu nome com o botão esquerdo do mouse. Neste momento serão mostrados os seus atributos nos campos após a listagem de usuários.
2. Altera-se o valor dos atributos desejados e clica-se no botão **Aplicar** ou no botão **OK**. A partir deste momento as alterações serão efetivadas.

Para se incluir um usuário na lista, deve-se proceder da seguinte forma:

1. Clica-se com o botão direito do mouse em qualquer lugar da área reservada para mostrar a lista (aparecerá o botão **Inserir**) e seleciona-se a opção **Incluir** no menu pop-up ou clica-se no ícone que representa a inclusão na barra de ferramentas.
2. Preenche-se os campos do usuário a ser incluído e clica-se no botão **Aplicar** ou no botão **OK**.

Para se remover um usuário da lista, deve-se proceder da seguinte forma:

1. Seleciona-se o usuário a ser removido, clicando sobre seu nome com o botão esquerdo do mouse, e clica-se no ícone que representa a remoção na barra de ferramentas.
   ou
2. Clica-se com o botão direito do mouse sobre o nome do usuário a ser removido e seleciona-se a opção **Excluir** no menu pop-up.

Significado dos atributos de um usuário

- **Login**

É a identificação do usuário para o firewall. Não podem existir dois usuários com o mesmo login. Este login será pedido ao administrador do firewall quando este for estabelecer uma sessão de administração remota.

O login deve ter entre 1 e 14 caracteres. Não há diferenças entre letras maiúsculas e minúsculas neste campo.

- **Nome**

Este campo contém o nome completo do usuário associado ao login. Ele tem objetivos puramente informacionais, não sendo usado para qualquer validação.

Este nome deve ser um conjunto de caracteres de comprimento entre 0 e 40.

- **Senha**

Este campo será usado em conjunto com o campo login para identificar um usuário perante o Firewall Aker. Ao se digitar a senha, serão mostrados na tela asteriscos "*" ao invés das letras.

O campo senha deve ter no máximo 14 caracteres. Seu tamanho mínimo é configurável através da janela de parâmetros da interface (para maiores informações veja o tópico Configurando os parâmetros da interface). **Neste campo, letras maiúsculas e minúsculas são consideradas diferentes.**

É extremamente importante que as senhas usadas tenham um comprimento grande, o mais próximo possível do limite de 14 caracteres. Além disso, deve-se sempre utilizar uma combinação de letras minúsculas, maiúsculas, números e caracteres especiais nas senhas (caracteres especiais são aqueles encontrados no teclado dos computadores e que não são números nem letras: "$", "&", "]", etc). Nunca use como senhas palavras em qualquer idioma ou apenas números.

- **Confirmação**

Este campo serve para que se confirme a senha digitada no campo anterior, uma vez que esta aparece como asteriscos.

- **Permissões**

Este campo define o que um usuário pode fazer dentro do Firewall Aker. Ele consiste de três opções que podem ser marcadas independentemente.

O objetivo destas permissões é possibilitar a criação de uma administração descentralizada para o firewall. É possível por exemplo, numa empresa que possua vários departamentos e vários firewalls, deixar um administrador responsável pela configuração de cada um dos firewalls e um responsável central com a tarefa de supervisionar a administração. Este supervisor seria a única pessoa capaz de apagar e alterar a configuração de log e eventos dos firewalls. Desta forma, apesar de cada departamento ter autonomia de administração, é possível se ter um controle central do que cada administrador alterou na configuração e quando ele realizou cada alteração. Isto é um recurso muito importante para se realizar auditorias internas, além de aumentar a segurança da administração.

Caso um usuário não possua nenhum atributo de autoridade então este terá permissão apenas para visualizar a configuração do firewall e compactar os arquivos de log e de eventos.

- **Configuração do Firewall**

Se esta permissão estiver marcada, o usuário em questão poderá administrar o firewall, isto é, alterar a configuração das entidades, regras de filtragem, conversão de endereços, criptografia, proxies e parâmetros de configuração que não estejam relacionados ao log.

- **Configuração do Log**

Se esta opção estiver marcada, o usuário em questão terá poderes para alterar os parâmetros relacionados ao log (como por exemplo, tempo de permanência do log), alterar a configuração da janela de ações (tanto as mensagens quanto os parâmetros) e apagar permanentemente o log e os eventos.

- **Controle de Usuários**

Se esta opção estiver marcada, o usuário em questão terá acesso à janela de administração de usuários, podendo incluir, editar e excluir outros usuários.

Um usuário que possuir esta autoridade somente poderá criar, editar ou excluir usuários com autoridades iguais ou menores às que ele possuir (por exemplo, se um usuário tiver poderes de gerenciar usuários e configurar log, então ele poderá criar usuários que não possuam nenhuma autoridade, que somente possam configurar o log, que somente possam criar novos usuários ou que possam gerenciar usuários e configurar log. Ele não poderá nunca criar, nem editar ou excluir, um usuário que possa configurar o firewall)

- **Permitir conexões do gerenciador**

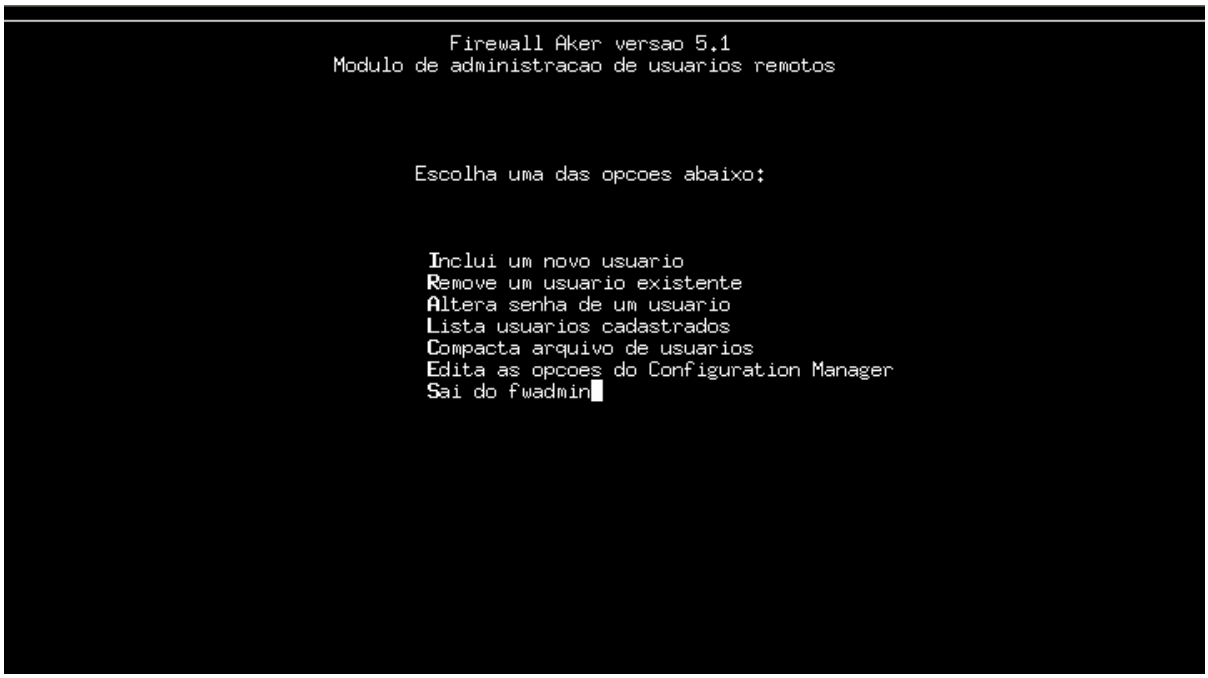
Essa opção permite habilitar/desabilitar acessos ao Firewall Aker pelo Configuration Manager. Ao habilitar conexões, é necessário informar a senha que será comum ao firewall e o gerenciador (shared secret).

3-2 Utilizando a interface texto

Além da interface gráfica de administração de usuários, existe uma interface local orientada à caracteres que possui praticamente as mesmas capacidades da interface gráfica. A única função não disponível é a de alteração das permissões dos usuários. Esta interface texto, ao contrário da maioria das demais interfaces orientadas à caracteres do Firewall Aker, é interativa e não recebe parâmetros da linha de comando.

Localização do programa: /etc/firewall/fwadmin

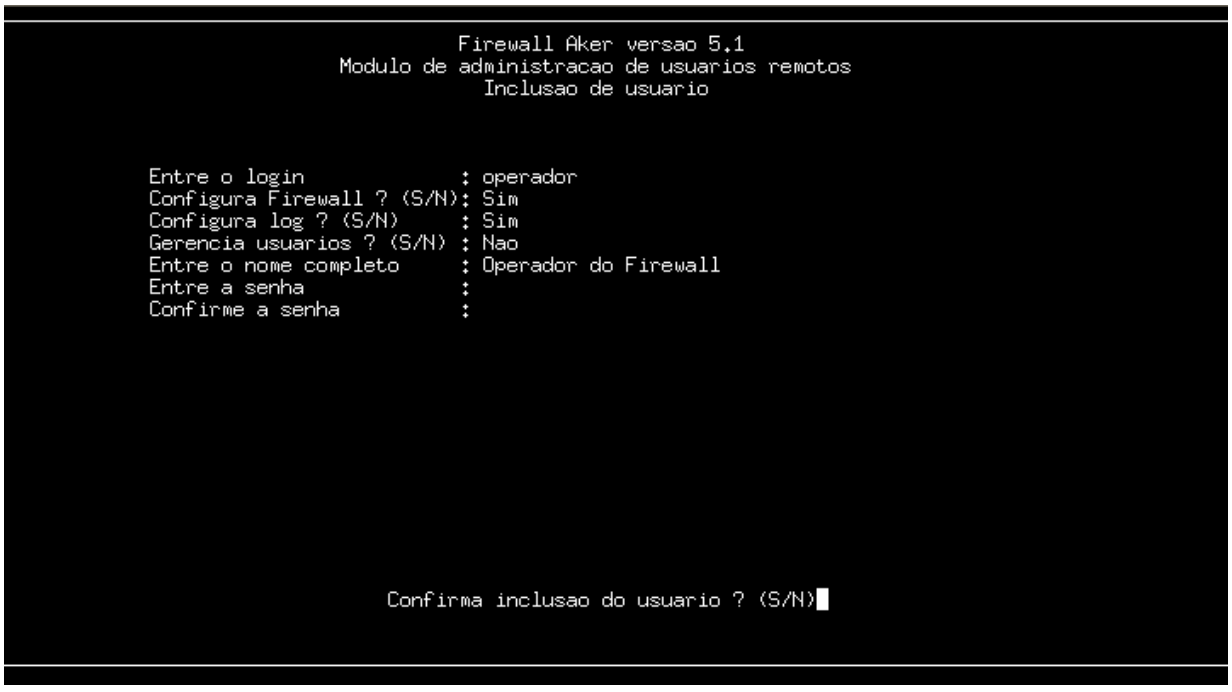
Ao ser executado, o programa mostrará a seguinte tela:


Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Escolha uma das opcoes abaixo:
Inclui um novo usuario
Remove um usuario existente
Altera senha de um usuario
Lista usuarios cadastrados
Compacta arquivo de usuarios
Edita as opcoes do Configuration Manager
Sai do fwadmin

Para executar qualquer uma das opções mostradas, basta se digitar a letra mostrada em negrito. Cada uma das opções será mostrada em detalhes abaixo:

- Inclui um novo usuário

Esta opção permite a inclusão de um novo usuário que poderá administrar o Firewall Aker remotamente. Ao ser selecionada, será mostrada uma tela pedindo as diversas informações do usuário. Após todas as informações serem preenchidas, será pedida uma confirmação para a inclusão do usuário.


Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Inclusao de usuario
Entre o login : operador
Configura Firewall ? (S/N): Sim
Configura log ? (S/N) : Sim
Gerencia usuarios ? (S/N) : Nao
Entre o nome completo : Operador do Firewall
Entre a senha :
Confirme a senha :
Confirma inclusao do usuario ? (S/N)

Observações importantes:

1. Nos campos onde aparecem as opções (S/N), deve-se digitar apenas S, para sim e N para não.
2. A senha e a confirmação das senhas não serão mostradas na tela.

- Remove um usuário existente

Esta opção remove um usuário que esteja cadastrado no sistema. Será pedido o login do usuário a ser removido. Se o usuário realmente estiver cadastrado, será pedida a seguir uma confirmação para realizar a operação.

Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Remocao de usuario
Entre o login : operador
Confirma remocao do usuario ? (S/N)

Para prosseguir com a remoção, deve-se digitar S, caso contrário digita-se N.

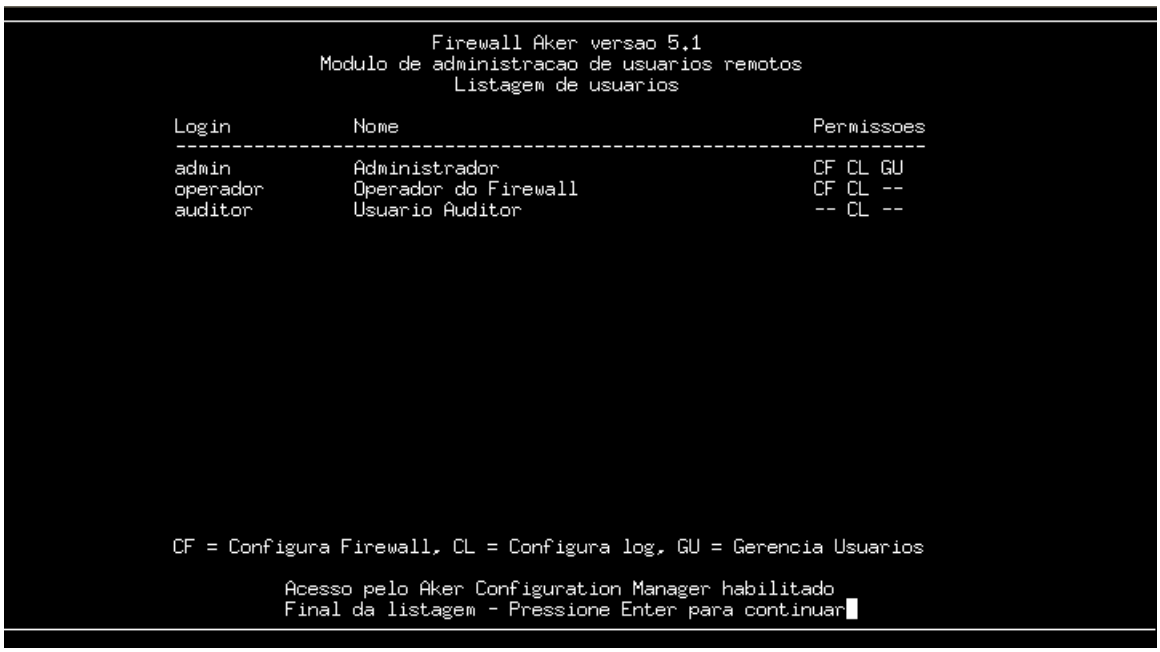
- Altera senha de um usuário

Esta opção permite com que se altere a senha de um usuário já cadastrado no sistema. Será pedido o login do usuário e caso este exista, serão pedidas a nova senha e a confirmação desta nova senha (conforme já comentado anteriormente, a senha e a confirmação não serão mostradas na tela).

Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Alteracao de senha de usuario
Entre o login : operador
Entre a nova senha :
Confirme a nova senha :
Senha alterada com sucesso - Pressione Enter

- Lista usuários cadastrados

Esta opção mostra uma lista com o nome e as permissões de todos os usuários autorizados a administrar remotamente o firewall. Um exemplo de uma possível listagem de usuários é a seguinte:


Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Listagem de usuarios
Login Nome Permissoes
admin Administrador CF CL GU
operador Operador do Firewall CF CL --
auditor Usuario Auditor -- CL --
CF = Configura Firewall, CL = Configura log, GU = Gerencia Usuarios
Acesso pelo Aker Configuration Manager habilitado
Final da listagem - Pressione Enter para continuar

O campo permissões consiste de 3 possíveis valores: CF, CL, e GU, que correspondem às permissões de Configura Firewall, Configura Log e Gerencia Usuários, respectivamente. Se um usuário possuir uma permissão, ela será mostrada com o código acima, caso contrário será mostrado o valor --, indicando que o usuário não a possui.

- Compacta arquivo de usuários

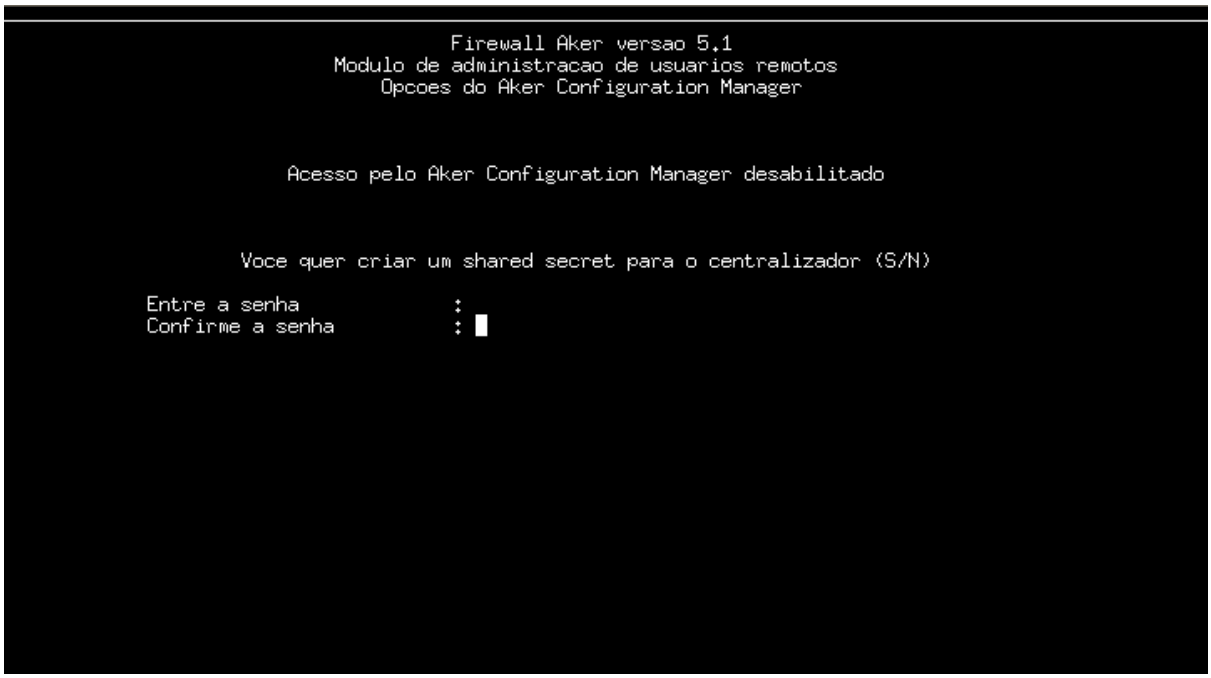
Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Compactacao do arquivo de usuarios
Compactando arquivo, aguarde...
Arquivo compactado com sucesso - Pressione Enter

Esta opção não está presente na interface gráfica e não possui uso freqüente. Ela serve para compactar o arquivo de usuários, removendo entradas não mais usadas. Ele somente deve ser usada quando for removido um grande número de usuários do sistema.

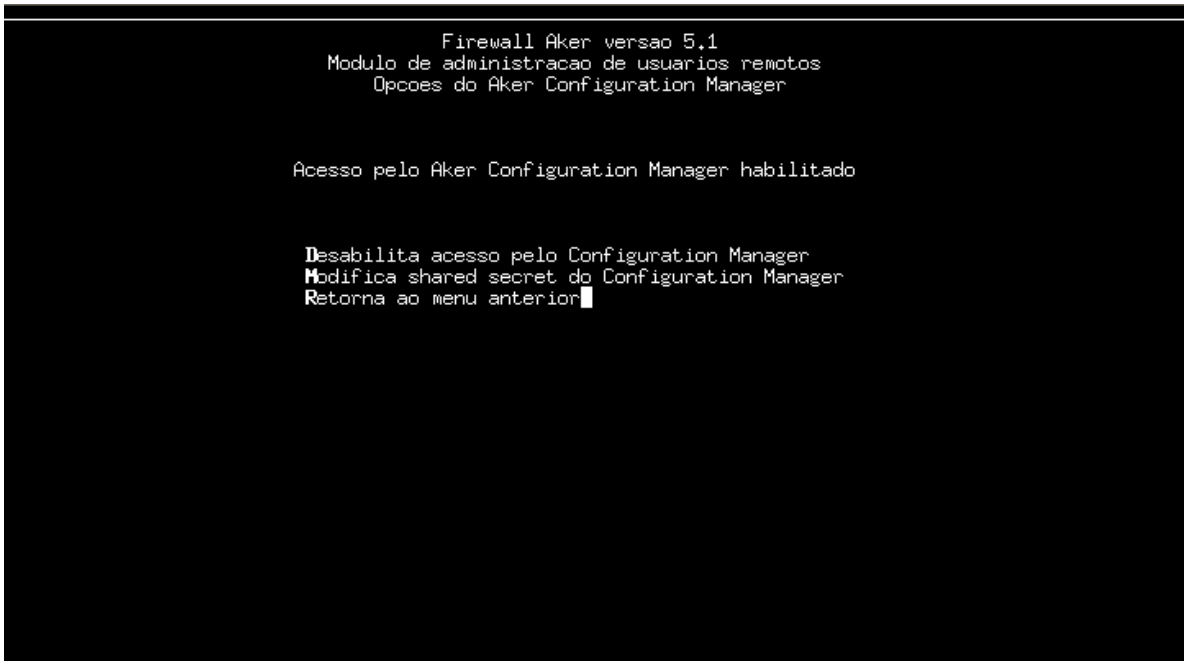
Ao ser selecionada, o arquivo será compactado e ao final será mostrada uma mensagem indicando que a operação foi completada (a compactação do arquivo costuma ser uma operação bastante rápida, durando poucos segundos).

- Edita as opções do Configuration Manager

Esta opção permite alterar as configurações do Aker Configuration Manager. É possível habilitar/desabilitar acessos ao Firewall Aker pelo Configuration Manager e modificar a shared secret. Se o acesso ao firewall não estiver habilitado, será mostrada uma tela pedindo a criação da shared secret. É necessário preencher a senha e sua confirmação. Essas não serão mostradas.


Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Opcoes do Aker Configuration Manager
Acesso pelo Aker Configuration Manager desabilitado
Voce quer criar um shared secret para o centralizador (S/N)
Entre a senha :
Confirme a senha :

Se o acesso ao firewall já estiver habilitado, serão mostradas novas opções de configuração:


Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Opcoes do Aker Configuration Manager
Acesso pelo Aker Configuration Manager habilitado
Desabilita acesso pelo Configuration Manager
Modifica shared secret do Configuration Manager
Retorna ao menu anterior

- Desabilita acesso pelo Configuration Manager

Ao selecionar essa opção, não será mais possível acessar o Firewall Aker pelo Configuration Manager até que o usuário habilite o acesso novamente.

- Modifica shared secret do Configuration Manager

Permite alterar a shared secret. É necessário entrar com a nova senha e a confirmação da nova senha. A senha e sua confirmação não serão mostradas na tela.

Firewall Aker versao 5.1
Modulo de administracao de usuarios remotos
Alteracao de senha do Aker Configuration Manager
Entre a nova senha :
Confirme a nova senha :
Senha alterada com sucesso - Pressione Enter

- Sai do fwadmin

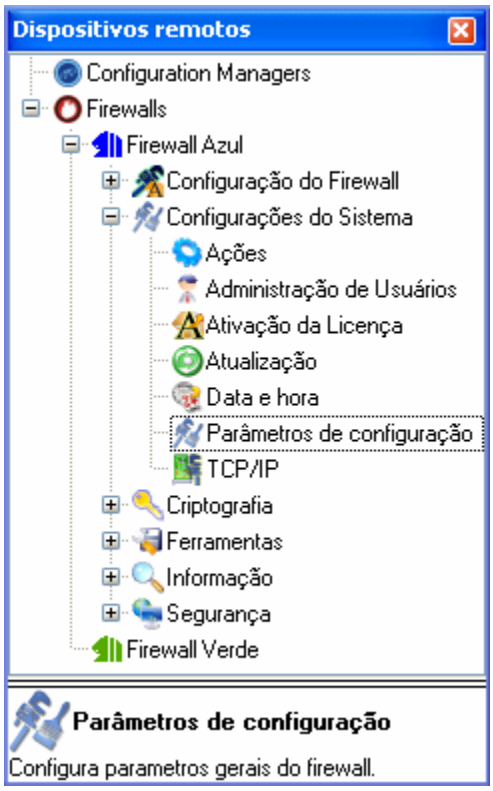
Esta opção encerra o programa fwadmin e retorna para a linha de comando

4-0 Configurando os parâmetros do sistema

Neste capítulo mostraremos como configurar as variáveis que irão influenciar nos resultados de todo o sistema. Estes parâmetros de configuração atuam em aspectos como a segurança, log do sistema e tempos de inatividade das conexões.

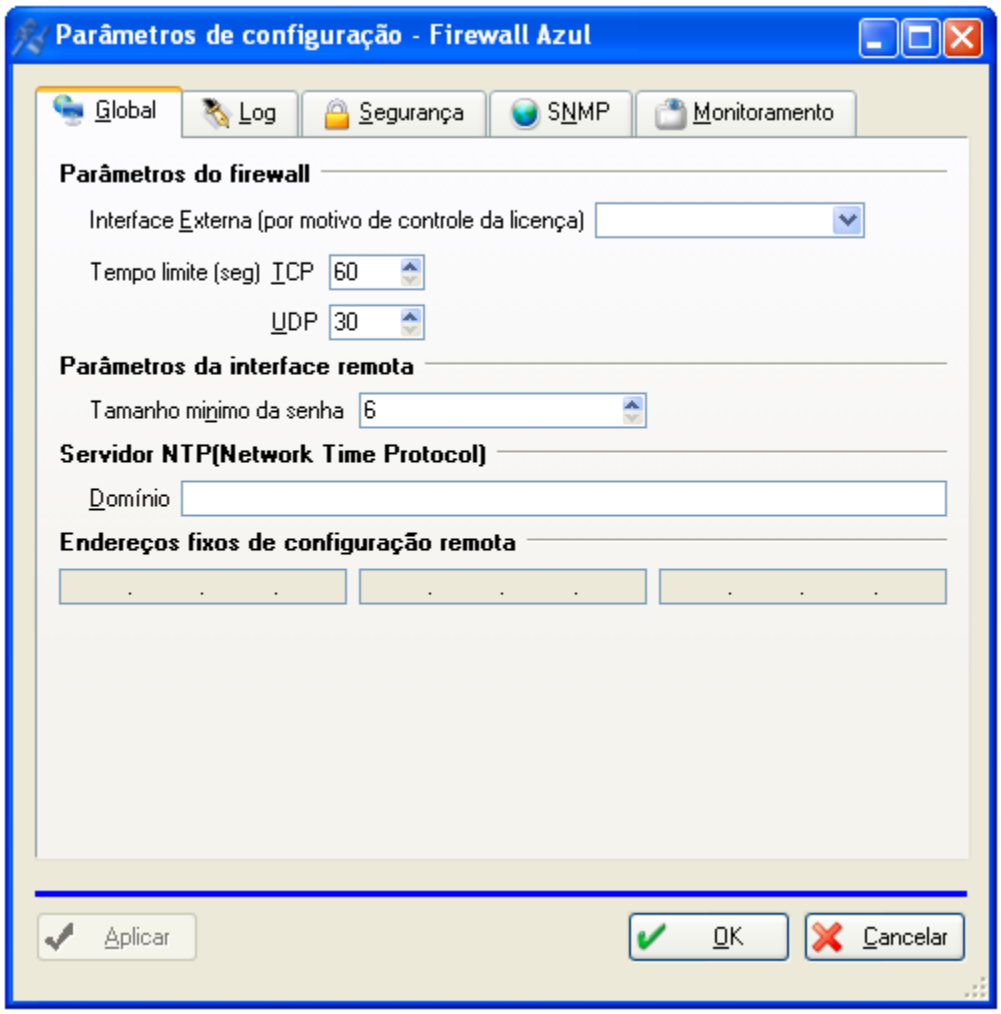
4-1 Utilizando a interface gráfica

Para ter acesso a janela de configuração de parâmetros basta:



- Clicar no menu *Configurações do Sistema* da janela do firewall que se quer administrar.
- Selecionar o item *Parâmetros de Configuração*

A janela de Parâmetros de configuração



- O botão **OK** fará com que a janela de configuração de parâmetros seja fechada e as alterações efetuadas aplicadas.
- O botão **Cancelar** fará com que a janela seja fechada porém as alterações efetuadas não sejam aplicadas.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

Significado dos parâmetros

- **Aba Global**

Nesta janela, estes parâmetros são utilizados pelo filtro de estados e pelo conversor de endereços. Eles consistem dos seguintes campos:

Interface Externa: Define o nome da interface externa do firewall. Conexões que vierem por esta interface não contarão na licença.

Valor padrão: Configurado durante a instalação do firewall pelo administrador.

Tempo limite TCP: Define o tempo máximo, em segundos, que uma conexão TCP pode permanecer sem tráfego e ainda ser considerada ativa pelo firewall. Seu valor pode variar de *0 a 30000*.

Valor padrão: ***900*** segundos.

Tempo limite UDP: Define o tempo máximo, em segundos, que uma conexão UDP pode permanecer sem tráfego e ainda ser considerada ativa pela firewall. Seu valor pode variar de *0* a *30000*.

Valor padrão: ***180*** segundos.

Estes campos são de vital importância para o correto funcionamento do firewall: valores muito altos poderão causar problemas de segurança para serviços baseados no protocolo UDP, farão com que o sistema utilize mais memória e o tornarão mais lento. Valores muito baixos poderão causar constantes quedas de sessão e o mau funcionamento de alguns serviços.

Tamanho mínimo de senha: Define o número mínimo de caracteres que as senhas dos administradores devem ter para serem aceitas pelo sistema. Seu valor pode variar entre 4 e 14 caracteres.

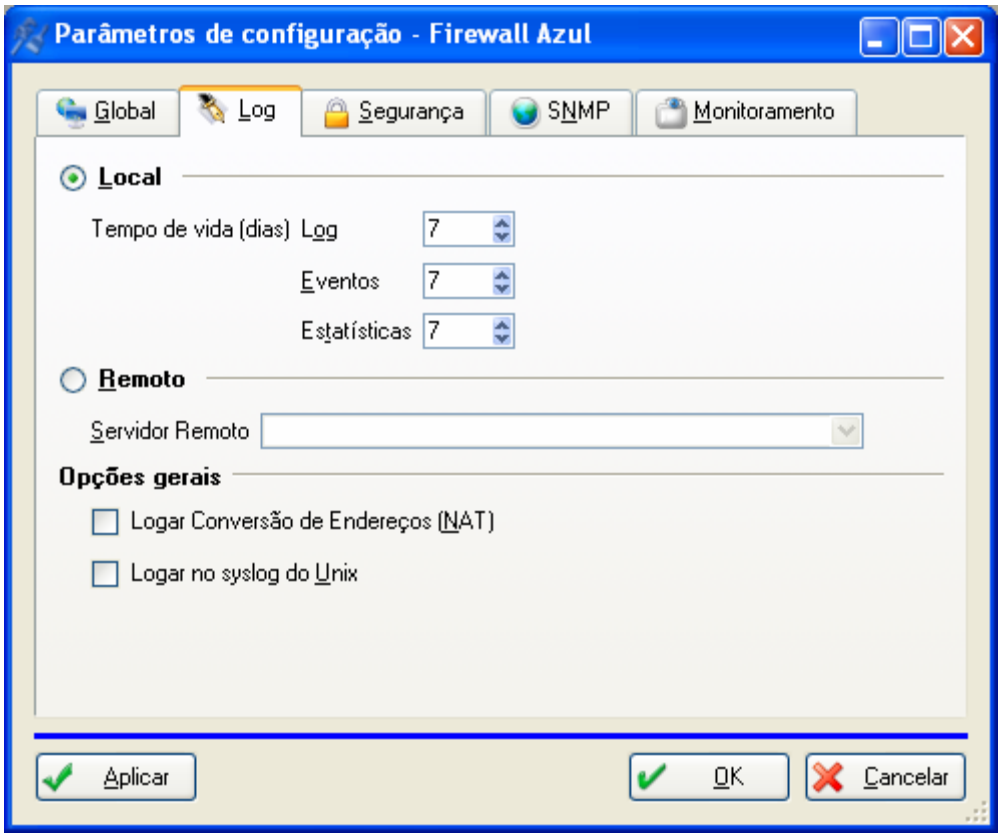
Valor padrão: **6** caracteres.

É importante que este valor seja o maior possível, de modo a evitar a utilização de senhas que possam ser facilmente quebradas.

Servidor NTP (Network Time Protocol): Define o servidor de tempo que será utilizado pelo firewall para sincronizar seu relógio interno. (Este campo só aparece para os Firewall Box)

Endereços fixos de configuração remota: São endereços que, independentemente de regras e de extrapolação dos limites de licenças, podem administrar o firewall (isto é conectar na porta 1020). Eles servem como medida de prevenção anti-bloqueio do firewall, uma vez que só podem ser configurados via interface texto.

- **Aba Log**



Local: Indica que o log/eventos/estatísticas devem ser salvos em um disco local, na máquina onde o firewall estiver rodando.

Tempo de vida no log / eventos / estatística: Os registros de log, eventos e estatísticas do firewall são mantidos em arquivos diários. Esta configuração define o número máximo de arquivos que serão mantidos pelo sistema, em caso de log local. Os valores possíveis vão de 1 a 365 dias.

Valor padrão: ***7*** dias

No caso de utilização de log remoto essas opções estarão desabilitadas e deverão ser configuradas no próprio servidor remoto

Remoto: Esta opção indica que o log/eventos/estatísticas deverão ser enviados para um servidor de log remoto ao invés de serem gravados no disco local. Com isso, o controle de diversos firewalls pode ser centralizado, facilitando a auditoria.

Servidor de Log Remoto: Esta opção indica o servidor de log remoto para o qual o log/eventos/estatísticas serão enviados.

Logar Tradução de Endereço de Rede (NAT): Habilita o registro no log do sistema das conversões de endereços feitas pelo firewall.

Valor padrão: ***Conversões de endereço não devem ser logadas***

Mesmo com esta opção ativa, somente serão logados os pacotes convertidos através das conversões 1:N e N:1. As conversões por outros tipos de regras não serão registradas.

A ativação desta opção não traz nenhuma informação importante e deve ser utilizada apenas para fim de testes ou para se tentar resolver problemas.

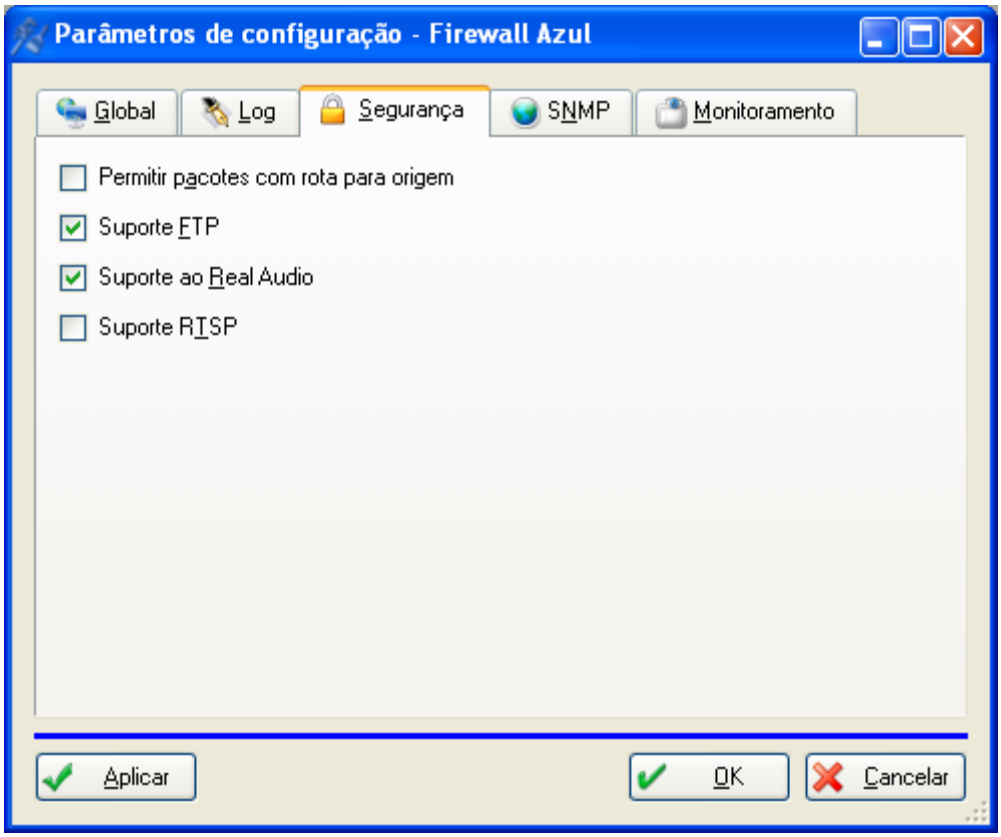
Logar syslog do Unix: Habilita o envio do log e dos eventos do firewall para o daemon de log do Unix, o *syslogd*.

Valor padrão: ***Não envia log para o syslogd***

Caso se habilite esta opção, os registros de log serão enviados para a fila *local0* e os de eventos para a fila *local1*.

Esta opção não altera em nada o registro interno do log e dos eventos realizado pelo próprio firewall.

- **Aba Segurança**



- **Parâmetros de Segurança**

Permitir pacotes com rota para origem: Habilita a passagem de pacotes que tenham a opção de registro de rota ou de roteamento dirigido. Se esta opção estiver desmarcada, pacotes com alguma destas opções não poderão trafegar.

Valor padrão: ***Pacotes IP direcionados não são permitidos.***

Cabe ressaltar que a aceitação de pacotes com qualquer uma das opções mostradas acima pode causar uma falha séria de segurança. A não ser que se tenha uma razão específica para deixá-los passar, deve-se manter esta opção desmarcada.

Suporte FTP: Habilita o suporte específico para o protocolo FTP.

Valor padrão: ***Suporte FTP está habilitado***

Este parâmetro faz com que o firewall trate o protocolo FTP de forma especial, de modo a permitir que ele funcione transparentemente para todas as máquinas clientes e servidoras, internas ou externas. A menos que não se pretenda usar FTP através do firewall, esta opção deve estar marcada.
Suporte ao Real Audio: Habilita o suporte para os protocolos Real Audio e Real Video.

Valor padrão: ***Suporte Real Audio está habilitado***

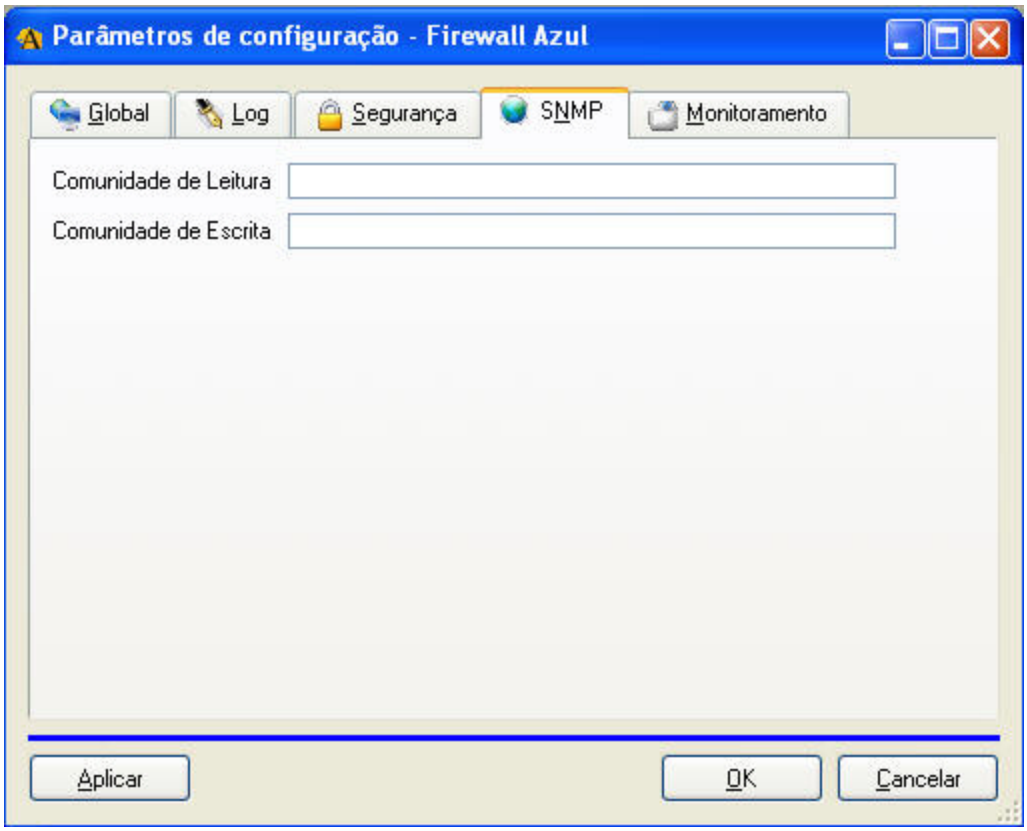
Este parâmetro faz com que o firewall trate o protocolo Real Audio / Real Video de forma especial, de modo a permitir que ele funcione transparentemente usando conexões TCP e UDP. A menos que não se pretenda usar o Real Audio ou se pretenda utilizá-lo apenas com conexões TCP, esta opção deve estar marcada.

Suporte RTSP: Habilita o suporte para o protocolo RTSP.

Valor padrão: ***Suporte RTSP está habilitado***

O RTSP (Real Time Streaming Protocol) é um protocolo que atua a nível de aplicação e ajuda a prover um certo arranjo que permite a entrega controlada de dados de tempo real, como áudio e vídeo. Fontes de dados podem incluir programas ao vivo (com áudio e vídeo) ou algum conteúdo armazenado (eventos pré-gravados). Ele é projetado para trabalhar com protocolos como o RTP, HTTP e/ou outro que de suporte a mídia continuas sobre a Internet. Ele suporta tráfego multicast bem como unicast. E também suporta interoperabilidade entre clientes e servidores de diferentes fabricantes. Este parâmetro faz com que o firewall trate o protocolo de forma especial, de modo a permitir que ele funcione transparentemente usando conexões TCP e UDP.

- **Aba SNMP**



- **Parâmetros de SNMP**

Comunidade de leitura: Este parâmetro indica o nome da comunidade que está autorizada a ler dados do firewall via SNMP. Caso este campo esteja em branco, nenhuma máquina estará autorizada a lê-los.

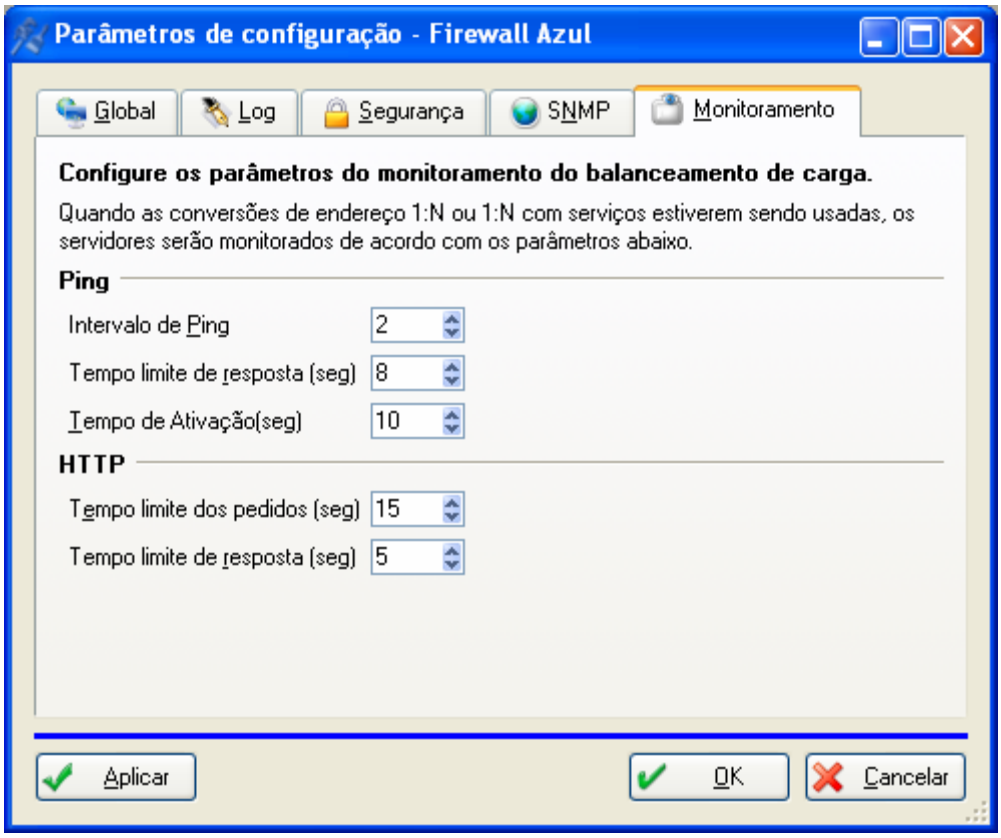
Valor padrão: ***campo em branco***

Comunidade de escrita: Este parâmetro indica o nome da comunidade que está autorizada a alterar dados do firewall via SNMP. Caso este campo esteja em branco, nenhuma máquina estará autorizada a alterá-los.

Valor padrão: ***campo em branco***

Mesmo com uma comunidade de escrita definida, por razões de segurança, somente poderão ser alterados algumas variáveis do grupo ***system***.

- **Aba Monitoramento**



Quando se utiliza conversão 1-N, ou seja, balanceamento de canal, é possível se configurar o tipo de monitoramento a ser realizado pelo firewall para verificar se as máquinas participantes do balanceamento estão no ar. Os parâmetros de monitoramento permitem que se modifique os intervalos de tempo de monitoramento, de modo a ajustá-los melhor a cada ambiente.

Monitoramento via ping

Esses parâmetros configuram os tempos utilizados pelo firewall para realizar o monitoramento via pacotes *ICMP Echo Request* e *Echo Reply*. São eles:

Intervalo de ping: Esse campo define de quanto em quanto tempo, em segundos, será enviado um ping para as máquinas sendo monitoradas. Seu valor pode variar entre 1 e 60 segundos.

Valor padrão: ***2*** segundos.

Tempo limite de resposta: Esse campo define o tempo máximo, em segundos, que uma máquina pode permanecer sem responder aos pacotes de ping enviados pelo firewall e ainda ser considerada ativa. Seu valor pode variar entre 2 e 120 segundos.

Valor padrão: ***8*** segundos.

Tempo de ativação: Esse campo define o tempo, em segundos, que o firewall irá esperar, após receber um pacote de resposta de uma máquina anteriormente fora do ar,

até considerá-la novamente ativa. Esse intervalo de tempo é necessário pois normalmente uma máquina responde a pacotes ping antes de estar com todos os seus serviços ativos. Seu valor pode variar entre 1 e 60 segundos.

Valor padrão: ***10*** segundos.

Monitoramento via http

Esses parâmetros configuram os tempos utilizados pelo firewall para realizar o monitoramento via requisições HTTP. São eles:

Tempo limite dos pedidos: Esse campo define de quanto em quanto tempo, em segundos, o firewall requisitará a URL especificada pelo administrador para cada máquina sendo monitorada. Seu valor pode variar entre 1 e 300 segundos.

Valor padrão: ***5*** segundos.

Tempo limite de resposta: Esse campo define o tempo máximo, em segundos, que uma máquina sendo monitorada poderá levar para responder à requisição do firewall e ainda ser considerada ativa. Seu valor pode variar entre 2 e 300 segundos.

Valor padrão: ***15*** segundos.

4-2 Utilizando a interface texto

A interface texto de configuração de parâmetros é bastante simples de ser utilizada e possui exatamente as mesmas capacidades da interface gráfica. Ela possui entretanto a possibilidade, não disponível na interface gráfica, de adicionar até três máquinas possíveis de administrarem o firewall remotamente, mesmo sem a existência de uma regra liberando sua conexão. O objetivo desta funcionalidade é permitir que, mesmo que um administrador tenha feito uma configuração equivocada que impeça sua conexão, ainda assim ele poderá continuar administrando remotamente o firewall. Este parâmetro chama-se **end_remoto**.

Localização do programa: `/etc/firewall/fwpar`

Sintaxe:

```
fwpar - mostra/altera parametros de configuracao
Uso: fwpar [mostra | ajuda]
     fwpar interface_externa <nome>
     fwpar [tempo_limite_tcp | tempo_limite_udp] <segundos>
     fwpar [ip_direcionado] <sim | nao>
     fwpar [suporte_ftp | suporte_real_audio | suporte_rtsp] <sim |
nao>
     fwpar [loga_conversao | loga_syslog] <sim | nao>
     fwpar [permanencia_log | permanencia_event | permanencia_stat]
<dias>
     fwpar [serv_log_remoto <nome>]
     fwpar [end_remoto <n> <end>]
     fwpar [comunidade_leitura | comunidade_escrita] [nome]
     mostra             = mostra a configuracao atual
     ajuda              = mostra esta mensagem
     interface_externa  = configura o nome da interface externa
(conexoes que
                          vierem por esta interface nao contam na
licenca)
```

```
     tempo_limite_tcp   = tempo maximo de inatividade para conexoes
TCP
     tempo_limite_udp   = tempo maximo de inatividade para conexoes
UDP
     ip_direcionado     = aceita pacotes IP direcionados
     suporte_ftp        = habilita suporte ao protocolo FTP
     suporte_real_audio = habilita suporte ao procotolo Real Audio
     suporte_rtsp       = habilita suporte ao procotolo RTSP
     loga_conversao     = registra mensagens de conversao de enderecos
     loga_syslog        = envia mensagens de log e eventos para o
syslogd
     permanencia_log    = tempo de permanencia (dias) dos registros de
log
     permanencia_event  = tempo de permanencia (dias) dos registris de
eventos
     permanencia_stat   = tempo de permanencia (dias) das estatisticas
     serv_log_remoto    = servidor de log remoto (nome da entidade)
     end_remoto         = endereco dos tres controladores remotos
     comunidade_leitura = nome da comunidade de leitura para SNMP
     comunidade_escrita = nome da comunidade de escrita para SNMP
```

Exemplo 1: (visualizando a configuração)

```
# fwpar mostra
Parametros globais:
-------------------
tempo_limite_tcp  : 900 segundos
tempo_limite_udp  : 180 segundos
interface_externa : lnc0
Parametros de seguranca:
------------------------
ip_direcionado    : nao
suporte_ftp       : sim
suporte_real_audio: sim
suporte_rtsp      : sim
end_remoto        : 1) 10.0.0.1       2) 10.0.0.2       3)10.0.0.3
Parametros de configuracao de log:
----------------------------------
loga_conversao    : nao
loga_syslog       : nao
permanencia_log   : 7 dias
permanencia_event : 7 dias
permanencia_stat  : 7 dias
Parametros de configuracao de SNMP:
-----------------------------------
comunidade_leitura:
comunidade_escrita:
```

Exemplo 2: (habilitando pacotes IP direcionados)

```
#/etc/firewall/fwpar ip_direcionado sim
```

Exemplo 3: (configurando o nome da comunidade de leitura SNMP)

```
#/etc/firewall/fwpar comunidade_leitura public
```

Exemplo 4: (apagando o nome da comunidade de escrita SNMP)

```
#/etc/firewall/fwpar comunidade_escrita
```

5-0 Cadastrando Entidades

Mostraremos aqui o que são, para que servem e como se cadastrar entidades no Firewall Aker

5-1 Planejando a instalação

O que são e para que servem as entidades ?

Entidades são representações de objetos do mundo real para o Firewall Aker. Através delas, pode-se representar máquinas, redes, serviços a serem disponibilizados, entre outros.

A principal vantagem da utilização de entidades para representar objetos reais é que a partir do momento em que são definidas no Firewall, elas podem ser referenciadas como se fossem os próprios objetos, propiciando uma maior facilidade de configuração e operação. Todas as alterações feitas em uma entidade serão automaticamente propagadas para todos os locais onde ela é referenciada.

Pode-se definir, por exemplo, uma máquina chamada de **Servidor WWW**, com o endereço IP de **`10.0.0.1`**. A partir deste momento, não é mais necessário se preocupar com este endereço IP. Em qualquer ponto onde seja necessário referenciar esta máquina, a referência será feita pelo nome. Caso futuramente seja necessário alterar seu endereço IP, basta alterar a definição da própria entidade que o sistema automaticamente propagará esta alteração para todas as suas referências.

Definindo entidades

Antes de explicar como cadastrar entidades no Firewall Aker, é necessário uma breve explicação sobre os tipos de entidades possíveis e o que caracteriza cada uma delas.

Existem 6 tipos diferentes de entidades no Firewall Aker: máquinas, redes, conjuntos, serviços, autenticadores e interfaces.

As entidades do tipo máquina e rede, como o próprio nome já diz, representam máquinas individuais e redes, respectivamente; entidades do tipo conjunto representam uma coleção de máquinas e redes, em qualquer número; entidades do tipo serviço representam um serviço a ser disponibilizado através de um protocolo qualquer que rode em cima do IP; entidades do tipo autenticador representam um tipo especial de máquina que pode ser utilizada para realizar autenticação de usuários; por último, entidades do tipo interface representam uma interface de rede do firewall.

Por definição, o protocolo IP, exige que cada máquina possua um endereço diferente. Normalmente, estes endereços são representados da forma byte a byte, como por exemplo `172.16.17.3`. Desta forma, pode-se caracterizar unicamente uma máquina em qualquer rede IP, incluindo a Internet, com apenas seu endereço.

Para definir uma rede, é necessário uma máscara além do endereço IP. A máscara serve para definir quais bits do endereço IP serão utilizados para representar a rede (bits com valor 1) e quais serão utilizados para representar as máquinas dentro da rede (bits com valor 0). Assim, para representar a rede cujas máquinas podem assumir os endereços IP de `192.168.0.1` a `192.168.0.254`, deve-se colocar como rede o valor `192.168.0.0` e como máscara o valor `255.255.255.0`. Esta máscara significa que os 3 primeiros bytes serão usados para representar a rede e o último byte será usado para representar a máquina.

Para se verificar se uma máquina pertence a uma determinada rede, basta fazer um **E** lógico da máscara da rede, com o endereço desejado e comparar com o **E** lógico do endereço da rede com sua máscara. Se eles forem iguais, a máquina pertence à rede, caso contrário não. Vejamos dois exemplos:

Suponha que desejamos verificar se a máquina 10.1.1.2 pertence à rede 10.1.0.0, máscara 255.255.0.0. Temos:

```
10.1.0.0 E 255.255.0.0 = 10.1.0.0 (para a rede)
10.1.1.2 E 255.255.0.0 = 10.1.0.0 (para o endereço)
```

Temos então que os dois endereços são iguais após a aplicação da máscara, portanto a máquina 10.1.1.2 pertence à rede 10.1.0.0.

Suponha agora que desejamos saber se a máquina 172.16.17.4 pertence à rede 172.17.0.0, máscara 255.255.0.0. Temos:

```
172.17.0.0 E 255.255.0.0 = 172.17.0.0 (para a rede)
172.16.17.4 E 255.255.0.0 = 172.16.0.0 (para o endereço)
```

Como os endereços finais são diferentes, temos que a máquina 172.16.17.4 não pertence à rede 172.17.0.0

Caso seja necessário definir uma rede onde qualquer máquina seja considerada como pertencente a ela (ou para especificar qualquer máquina da Internet), basta-se colocar como endereço IP desta rede o valor **`0.0.0.0`** e como máscara o valor **`0.0.0.0`**. Isto é bastante útil na hora de se disponibilizar serviços *públicos*, onde todas as máquinas da Internet terão acesso.

Toda a vez que ocorre uma comunicação entre duas máquinas, usando o protocolo IP, estão envolvidos não apenas os endereços de origem e destino, mas também um protocolo de nível mais alto (nível de transporte) e algum outro dado que identifique a comunicação unicamente. No caso dos protocolos TCP e UDP (que são os dois mais utilizados sobre o IP), uma comunicação é identificada por dois números: a **Porta Origem** e a **Porta Destino**.

A porta destino é um número fixo que está associada, geralmente, a um serviço único. Assim, temos que o serviço Telnet está associado com o protocolo TCP na porta 23, o serviço FTP com o protocolo TCP na porta 21 e o serviço SNMP com o protocolo UDP na porta 161, por exemplo.

A porta origem é um número sequencial escolhido pelo cliente de modo a possibilitar que exista mais de uma sessão ativa de um mesmo serviço em um dado instante. Assim,

uma comunicação completa nos protocolos TCP e UDP pode ser representada da seguinte forma:

```
    10.0.0.1        1024    ->     10.4.1.2          23           TCP
-------------------------------------------------------------------
---
Endereço origem  Porta origem  Endereço destino  Porta destino
Protocolo
```

Para um firewall, a porta de origem não é importante, uma vez que ela é randômica. Devido a isso, quando se define um serviço, leva-se em consideração apenas a porta de destino.

Além dos protocolos TCP e UDP, existe um outro protocolo importante, o ICMP. Este protocolo é utilizado pelo próprio IP para enviar mensagens de controle, informar sobre erros e testar a conectividade de uma rede.

O protocolo ICMP não utiliza o conceito de portas. Ele usa um número que varia de 0 a 255 para indicar um **Tipo de Serviço**. Como o tipo de serviço caracteriza unicamente um serviço entre duas máquinas, ele pode ser usado como se fosse a porta destino dos protocolos TCP e UDP na hora de definir um serviço.

Por último, existem outros protocolos que podem rodar sobre o protocolo IP e que não são TCP, UDP ou ICMP. Cada um destes protocolos tem formas próprias para definir uma comunicação e nenhum deles é utilizado por um grande número de máquinas. Ainda assim, o Firewall Aker optou por adicionar suporte para possibilitar ao administrador controle sobre quais destes protocolos podem passar através do firewall e quais não.

Para entender como isso é feito, basta se saber que cada protocolo tem um número único que o identifica para o protocolo IP. Este número varia de 0 a 255. Desta forma, podemos definir serviços para outros protocolos usando o número do protocolo como identificação do serviço.

O que é Qualidade de Serviço (QoS)

Qualidade de serviço pode ser compreendida de duas formas: do ponto de vista da aplicação ou da rede. Para uma aplicação, oferecer seus serviços com qualidade significa atender às expectativas, muitas vezes subjetivas, do usuário em termos do tempo de resposta e da qualidade do serviço que está sendo provido. Por exemplo, no caso de uma aplicação de vídeo, fidelidade adequada do som e/ou da imagem sem ruídos nem congelamentos.

A qualidade de serviço da rede depende das necessidades da aplicação, ou seja, do que ela requisita da rede a fim de que funcione bem e atenda, por sua vez, às necessidades do usuário. Estes requisitos são traduzidos em parâmetros indicadores do desempenho da rede como, por exemplo, o atraso máximo sofrido pelo tráfego da aplicação entre o computador origem e destino.

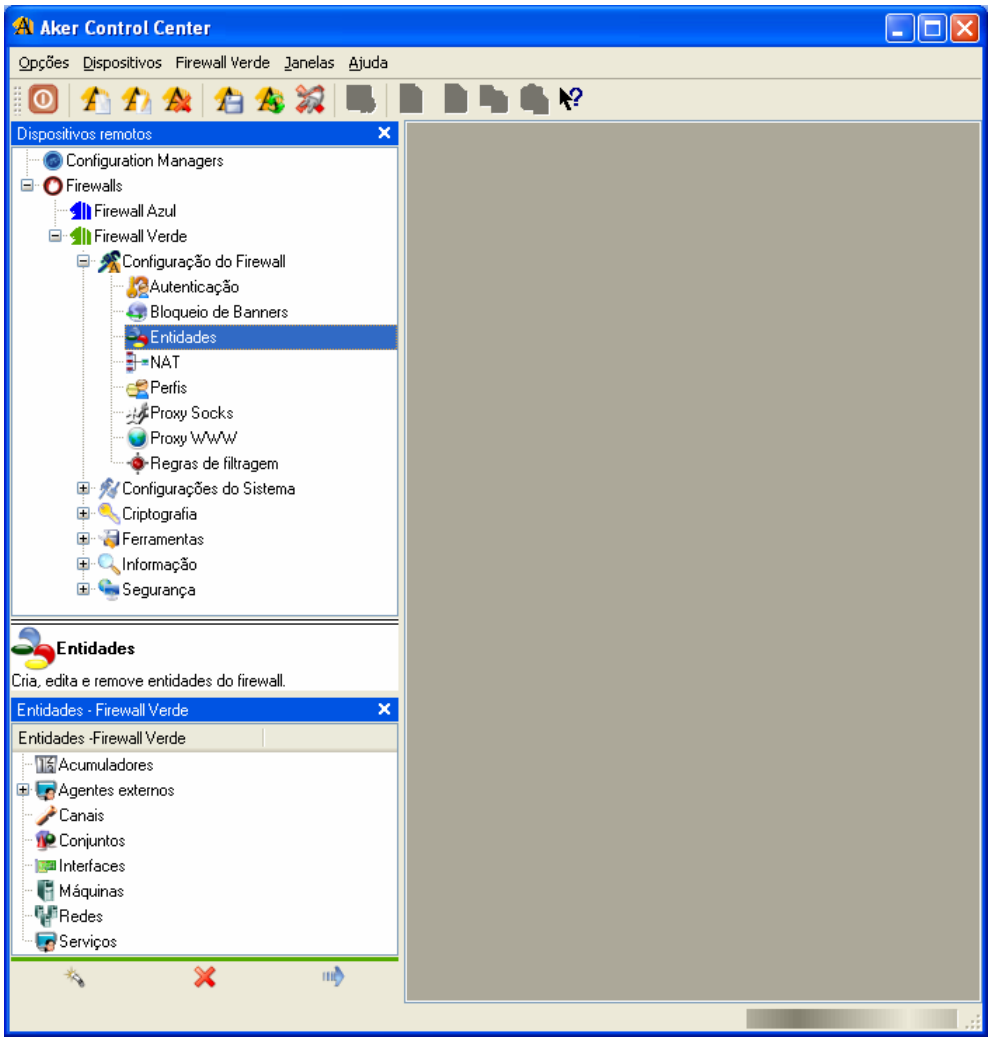
O Firewall Aker implementa um mecanismo com o qual é possível se definir uma banda máxima de tráfego para determinadas aplicações. Através de seu uso, determinadas

aplicações que tradicionalmente consomem muita banda, podem ter seu uso controlado. As entidades do tipo Canal são utilizadas para este fim e serão explicadas logo abaixo.

5-2 Cadastrando entidades utilizando a interface gráfica

Para ter acesso à janela de cadastro de entidades basta:

- Clicar no meu Configuração do Firewall da janela do firewall que se quer administrar;
- Selecionar o item *Entidades* (a janela será mostrada abaixo da janela com os menus de configuração dos firewalls).



A janela de cadastro de entidades

A janela de cadastro de entidades é onde são cadastradas todas as entidades do Firewall Aker, independente do seu tipo. Esta janela, por ser constantemente utilizada em praticamente todas as demais configurações do firewall, normalmente é mostrada sempre aberta, abaixo da janela com os menus de configuração de cada firewall.

Dica: É possível se posicionar a janela de entidades como se fosse uma janela comum, bastando para isso clicar sobre sua barra de título e arrastá-la para a posição desejada.

Nesta janela estão desenhados oito ícones, em forma de árvore, que representam os oito tipos de entidades possíveis de serem criados.

Dica: Para visualizar as entidades criadas é só clicar no sinal de + e as entidades ficarão listadas logo abaixo do logotipo.
Para se cadastrar uma nova entidade, deve-se proceder da seguinte forma:

1. Clica-se uma vez no ícone correspondente à entidade do tipo que se deseja criar com o botão direito do mouse e seleciona-se a opção **Inserir** no menu pop-up
   ou
2. Clica-se no ícone correspondente à entidade do tipo que se deseja criar e pressiona-se a tecla *Insert*.

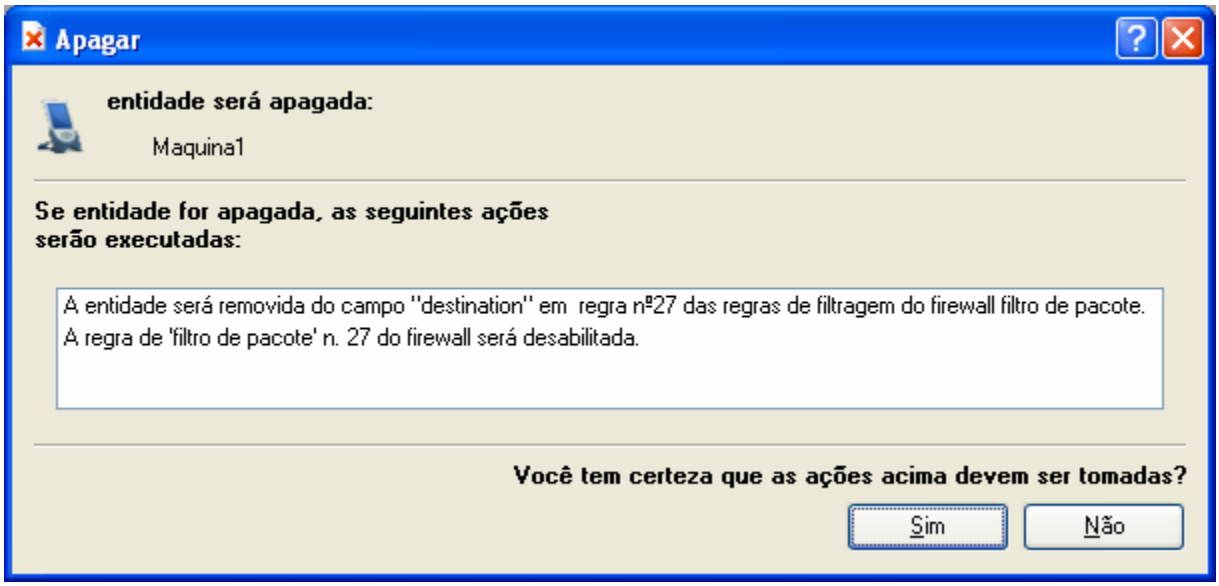
Para se editar ou excluir uma entidade, deve-se proceder da seguinte forma:

1. Seleciona-se a entidade a ser editada ou excluída (se necessário, expande-se a lista do tipo de entidade correspondente)
2. Clica-se com o botão direito do mouse e seleciona-se a opção **Editar** ou **Apagar**, respectivamente, no menu pop-up que aparecer.
   ou
3. Clica-se no ícone correspondente à entidade do tipo que se deseja criar e pressiona-se a tecla *Delete*.

No caso das opções *Editar* ou *Incluir*, aparecerá a janela de edição de parâmetros da entidade a ser editada ou incluída. Esta janela será diferente para cada um dos tipos possíveis de entidades.

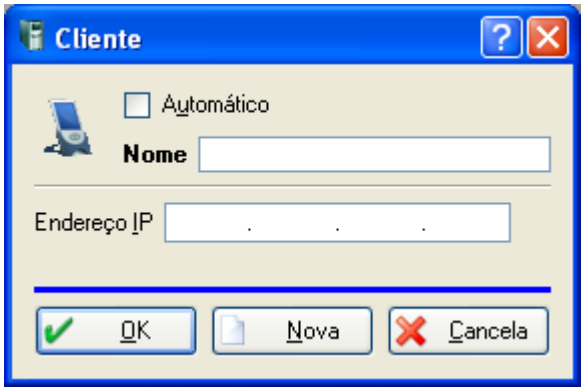
O ícone , localizado na parte inferior da janela aciona o assistente de cadastramento de entidades que será descrito no final deste capítulo.

A janela de alerta de exclusão de entidades


Apagar
entidade será apagada:
Maquina1
Se entidade for apagada, as seguintes ações serão executadas:
A entidade será removida do campo "destination" em regra nº27 das regras de filtragem do firewall filtro de pacote.
A regra de 'filtro de pacote' n. 27 do firewall será desabilitada.
Você tem certeza que as ações acima devem ser tomadas?
Sim
Não

Sempre que uma entidade estiver prestes a ser apagada, o sistema irá checar se existe alguma dependência da mesma na configuração, de modo a manter a integridade do firewall. Se existir qualquer dependencia, será mostrada uma lista de ações que serão executadas automaticamente pelo sistema, de modo a possibilitar que o administrador decida se quer proceder ou não com a remoção.

Incluindo / editando máquinas



Para se cadastrar uma entidade do tipo máquina, é necessário preencher os seguintes campos:

Nome: É o nome através do qual a máquina será referenciada daqui em diante pelo firewall. É possível se especificar este nome manualmente ou deixar que o ele seja atribuído automaticamente. A opção **Automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Letras maiúsculas e minúsculas são consideradas diferentes nos nomes das entidades. Desta forma, é possível a existência de várias entidades compostas de nomes com as mesmas letras, porém com combinações distintas de maiúsculas e minúsculas. As entidades **Aker**, **AKER** e **aker** são, portanto, consideradas diferentes.

Ícone: É o ícone que aparecerá associado à máquina em todas as referências. Para alterá-lo, basta clicar sobre o desenho do ícone atual. O firewall então mostrará uma lista com todos os possíveis ícones para representar máquinas. Para escolher entre eles basta clicar no ícone desejado e no botão **OK**. Caso não se deseje alterá-lo após ver a lista, basta clicar no botão **Cancelar**.

IP: É o endereço IP da máquina a ser criada.

Após todos os campos estarem preenchidos, deve-se clicar no botão **OK** para realizar a inclusão ou alteração da máquina. Para cancelar as alterações realizadas ou a inclusão, deve-se pressionar o botão **Cancelar**.

Para facilitar a inclusão de várias máquinas seguidamente, existe um botão chamado **Nova** (que não estará habilitado durante uma edição). Ao ser clicado, este botão fará com que a máquina cujos dados foram preenchidos seja incluída e a janela de inclusão de máquinas mantida aberta, pronta para uma nova inclusão. Desta forma, é possível se cadastrar rapidamente um grande número de máquinas.

Incluindo / editando redes

Para se cadastrar uma entidade do tipo rede, é necessário preencher os seguintes campos:
Nome: É o nome através do qual a rede será referenciada daqui em diante pelo firewall. É possível se especificar este nome manualmente ou deixar que o ele seja atribuído automaticamente. A opção **Automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Letras maiúsculas e minúsculas são consideradas diferentes nos nomes das entidades. Desta forma, é possível a existência de várias entidades compostas de nomes com as

mesmas letras, porém com combinações distintas de maiúsculas e minúsculas. As entidades **Aker**, **AKER** e **aker** são, portanto, consideradas diferentes.

Ícone: É o ícone que aparecerá associado à rede em todas as referências. Para alterá-lo, basta clicar sobre o desenho do ícone atual. O firewall então mostrará uma lista com todos os possíveis ícones para representar redes. Para escolher entre eles basta clicar no ícone desejado e no botão **OK**. Caso não se deseje alterá-lo após ver a lista, basta clicar no botão **Cancelar**.

IP: É o endereço IP da rede a ser criada.

Máscara: É a máscara da rede a ser definida.

Intervalo: Este campo mostra a faixa de endereço IP a que pertence a rede e realiza uma crítica quanto a máscara que está sendo cadastrada, ou seja não permite cadastramento de máscaras erradas.

Após todos os campos estarem preenchidos, deve-se clicar no botão **OK** para realizar a inclusão ou alteração da rede. Para cancelar as alterações realizadas ou a inclusão, deve-se pressionar o botão **Cancelar**.

Para facilitar a inclusão de várias redes seguidamente, existe um botão chamado **Nova** (que não estará habilitado durante uma edição). Ao ser clicado, este botão fará com que a rede cujos dados foram preenchidos seja incluída e a janela de inclusão de redes mantida aberta, pronta para uma nova inclusão. Desta forma, é possível se cadastrar rapidamente um grande número de redes.

Incluindo / editando conjuntos

Para se cadastrar uma entidade do tipo conjunto, é necessário preencher os seguintes campos:

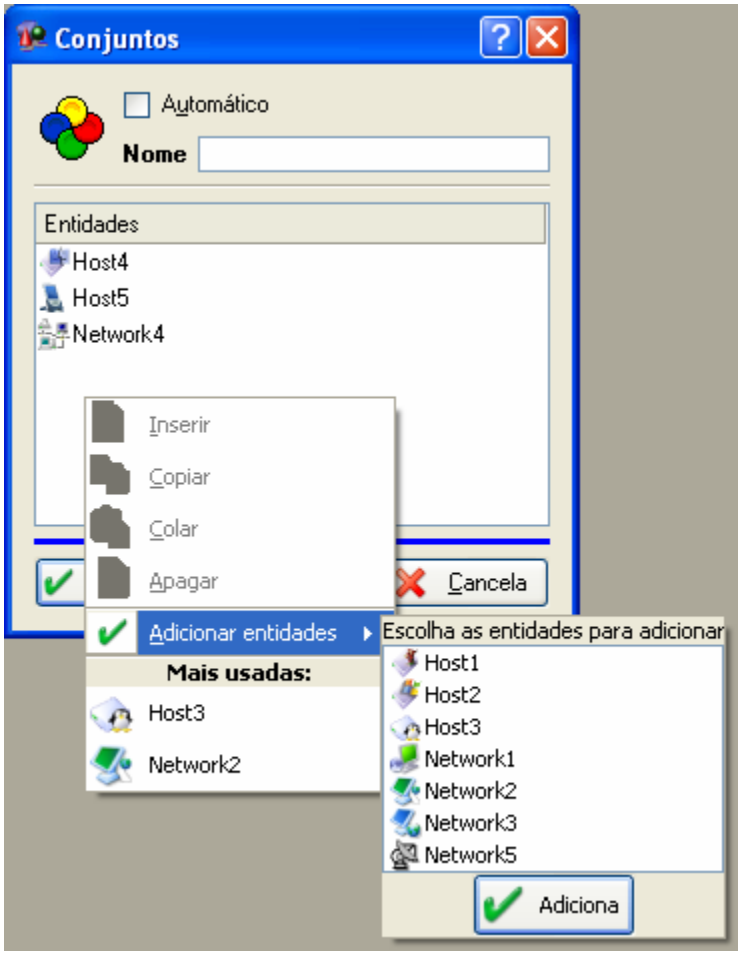
Nome: É o nome através do qual o conjunto será referenciado daqui em diante pelo firewall. É possível se especificar este nome manualmente ou deixar que ele seja atribuído automaticamente. A opção **Automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Letras maiúsculas e minúsculas são consideradas diferentes nos nomes das entidades. Desta forma, é possível a existência de várias entidades compostas de nomes com as mesmas letras, porém com combinações distintas de maiúsculas e minúsculas. As entidades **Aker**, **AKER** e **aker** são, portanto, consideradas diferentes.

Ícone: É o ícone que aparecerá associado ao conjunto em todas as referências. Para alterá-lo, basta clicar sobre o desenho do ícone atual. O firewall então mostrará uma lista com todos os possíveis ícones para representar conjuntos. Para escolher entre eles basta clicar no ícone desejado e no botão **OK**. Caso não se deseje alterá-lo após ver a lista, basta clicar no botão **Cancelar**.

Após preencher o nome e escolher o ícone para o conjunto, é necessário se definir quais máquinas e redes farão parte do mesmo, através dos seguintes passos:

1. Clica-se com o botão direito do mouse no campo em branco e seleciona-se a opção **Adicionar Entidades** (a entidade pode ser adicionada clicando-se duas vezes sobre ela ou clicando uma vez e logo abaixo em **Adicionar**).
   ou
2. Clica-se e sobre a entidade que se desejar incluir, arrasta-se e solta-se ela dentro da janela de entidades do conjunto.



Para se remover uma rede ou máquina do conjunto, deve-se proceder da seguinte forma:

1. Clica-se com o botão direito do mouse sobre a entidade a ser removida e seleciona-se a opção **Remover**.
   ou
2. Clica-se na máquina ou rede a ser removida e pressiona-se a tecla *Delete*.

Após todos os campos estarem preenchidos e todas as redes e máquinas que devem fazer parte do conjunto selecionadas, deve-se clicar no botão **OK** para realizar a inclusão ou alteração do conjunto. Para cancelar as alterações realizadas ou a inclusão, deve-se pressionar o botão **Cancelar**.

Para facilitar a inclusão de vários conjuntos seguidamente, existe um botão chamado **Nova** (que não estará habilitado durante uma edição). Ao ser clicado, este botão fará com que o conjunto cujos dados foram preenchidos seja incluído e a janela de inclusão de conjuntos mantida aberta, pronta para uma nova inclusão. Desta forma, é possível se cadastrar rapidamente um grande número de conjuntos.

Incluindo / Editando agentes externos

Agentes externos são utilizados para a definição de programas complementares ao Firewall Aker, responsáveis por funções específicas, que podem estar rodando em máquinas distintas. Quando houver necessidade de realização de uma determinada

tarefa por um dos agentes externos, ou vice-versa, o firewall se comunicará com eles e requisitará sua execução.

Existem 8 diferentes tipos de agentes externos, cada um responsável por um tipo distinto de tarefas:

- **Agentes Antivírus**

Os agentes antivírus são utilizados pelo proxy SMTP, POP3 e Proxy WWW para realizar a checagem e desinfecção de virus de forma transparente em e-mails e nos downloads FTP e HTTP.

- **Agentes IDS**

Os agentes IDS (Intrusion Detection Systems - Sistemas detetores de intrusão) são sistemas que ficam monitorando a rede em tempo real procurando por padrões conhecidos de ataques ou abusos. Ao detectar uma destas ameaças, ele pode incluir uma regra no firewall que bloqueará imediatamente o acesso do atacante.

- **Analisadores de contexto**

Os analisadores de contexto são utilizados pelo proxy WWW para controlar o acesso a URLs baseados em diversas categorias pré-configuradas.

- **Autenticadores**

Os agentes de autenticação são utilizados para se fazer autenticação de usuários no firewall utilizando usuarios/senhas de bases de dados de diversos sistemas operacionais (Windows NT, Linux, etc).

- **Autenticador Radius**

O autenticador Radius são utilizados para se fazer autenticação de usuários no firewall a partir de uma base Radius.

- **Autenticadores Token**

Os autenticadores token são utilizados para se fazer autenticação de usuários no firewall utilizando SecurID(R) , Alladin e outros.

- **Autoridade certificadora**

Autoridades certificadoras são utilizadas para se fazer autenticação de usuários através de PKI, com o uso de Smart Cards e para autenticação de firewalls com criptografia IPSEC.

- **Autenticadores LDAP**

O autenticador LDAP permite ao firewall autenticar usuário usando uma base LDAP compatível com o protocolo X500.

- **Servidor de log remoto**

Os servidores de log remoto são utilizados pelo firewall para enviar o log para armazenamento em uma máquina remota.

É possível a instalação de diversos agentes externos em uma mesma máquina, desde que cada um seja de um tipo distinto.

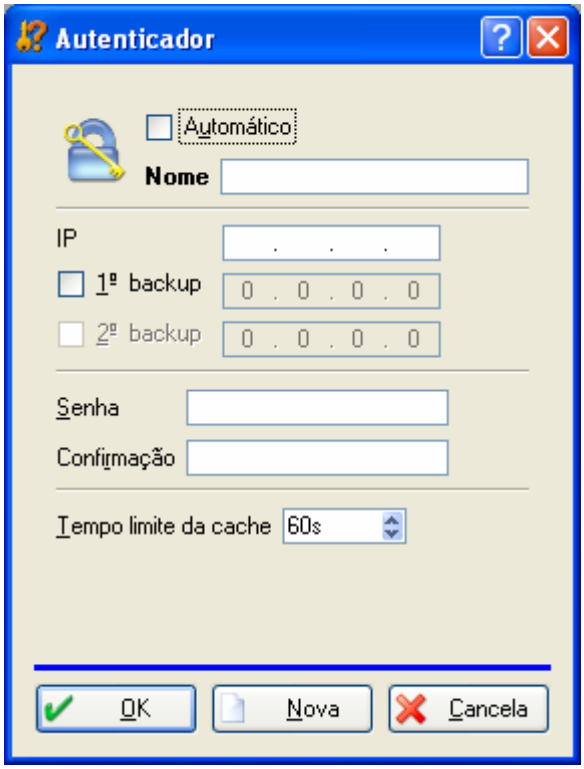
Para se cadastrar um agente externo deve-se inicialmente selecionar seu tipo, abrindo o diretório de Agentes Externos. Independemente de seu sub-tipo, todos os agentes externos possuem os seguintes campos (os demais campos serão então modificados de acordo com o tipo do agente a ser cadastrado):

Nome: É o nome através do qual o agente será referenciado daqui em diante pelo firewall. É possível se especificar este nome manualmente ou deixar que o ele seja atribuído automaticamente. A opção **Automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Letras maiúsculas e minúsculas são consideradas diferentes nos nomes das entidades. Desta forma, é possível a existência de várias entidades compostas de nomes com as mesmas letras, porém com combinações distintas de maiúsculas e minúsculas. As entidades **Aker**, **AKER** e **aker** são, portanto, consideradas diferentes.

Ícone: É o ícone que aparecerá associado ao agente em todas as referências. Para alterá-lo, basta clicar sobre o desenho do ícone atual. O firewall então mostrará uma lista com todos os possíveis ícones para representar agentes do sub-tipo selectionado. Para escolher entre eles basta clicar no ícone desejado e no botão **OK**. Caso não se deseje alterá-lo após ver a lista, basta clicar no botão **Cancelar**.

- Para se cadastrar um agente externo do tipo **Autenticador** ou **Autenticador Token**, é necessário preencher os seguintes campos adicionais:



IP: É o endereço IP da máquina onde o agente está rodando.

Backup e **Backup 2**: Estes campos permitem com que se especifique até dois endereços de outras máquinas que também estarão rodando o agente e que servirão como backup no caso de quedas da máquina principal.

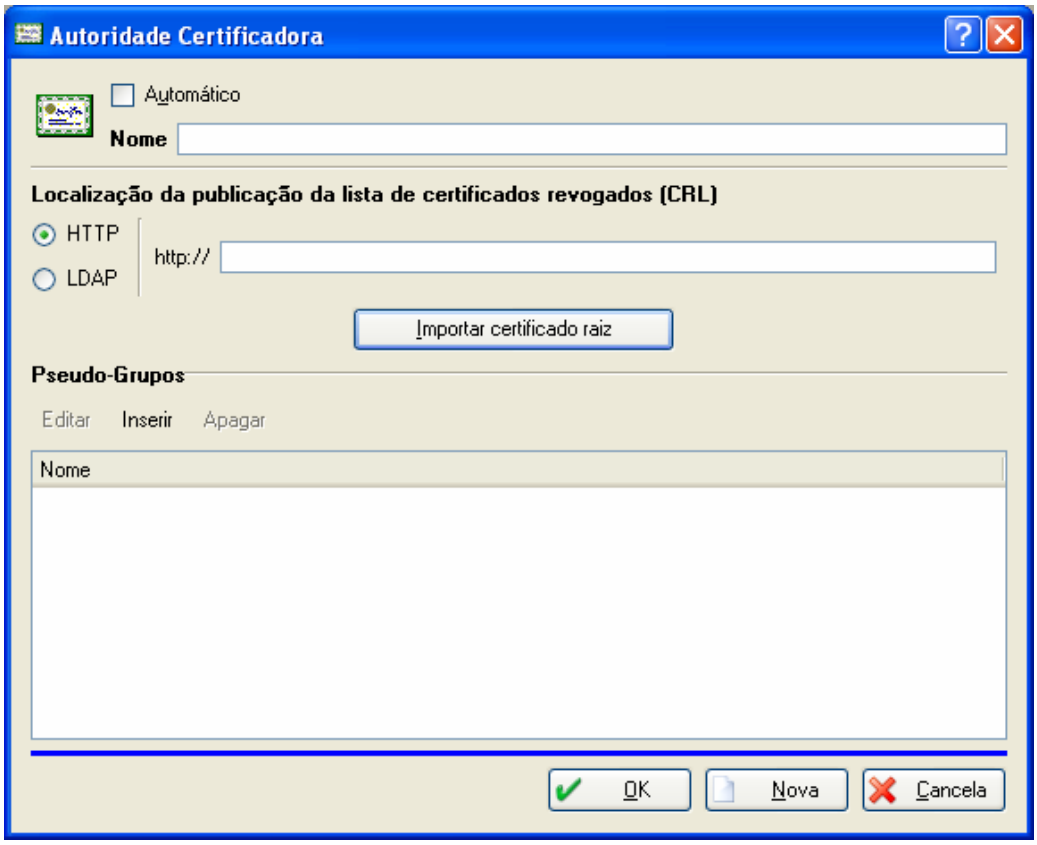
A máquina principal e as de backup deverão compartilhar uma mesma base de usuários, ou seja, elas deverão ser controladoras de domínio primárias e de backup (PDCs e BDCs), no caso de redes Windows, ou várias máquinas Unix utilizando NIS.
Senha: É a senha utilizada para gerar as chaves de autenticação e criptografia usadas na comunicação com o agente. Esta senha deve ser igual à configurada no agente. Para maiores informações, veja o capítulo intitulado Trabalhando com proxies.

Confirmação: Este campo é utilizado apenas para se verificar se a senha foi digitada corretamente. Deve-se digitá-la exatamente como no campo *Senha*.

Tempo limite de uso da cache: Todas as vezes que realiza uma autenticação com sucesso, o firewall mantém em memória os dados recebidos do usuário e do agente. Nas autenticações seguintes, o firewall possui todos os dados necessários e não mais precisa consultar o agente. Isso permite um grande ganho de performance.

Este parâmetro permite definir o tempo, em segundos, que o firewall deve manter as informações de autenticação em memória. Para maiores informações, veja o capítulo intitulado Trabalhando com proxies.

- Para se cadastrar um agente externo do tipo **Autoridade Certificadora**, é necessário preencher os seguintes campos adicionais:



Localização da publicação da lista de certificados revogados (CRL): É a URL da qual será baixada a lista de certificados revogados da CA (CRL). Esta URL deve ser obrigatoriamente do protocolo HTTP e deve ser especificada sem o http:// na sua frente.

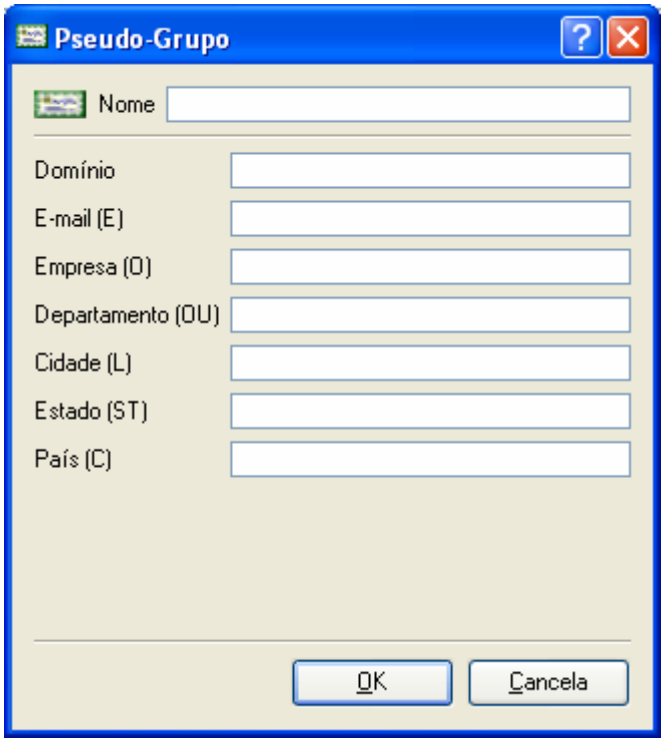
O botão **Importar certificado raiz** permite com que se carregue o certificado root da CA no firewall. Ao ser clicado, a interface abrirá uma janela para que se especifique o nome do arquivo com o certificado a ser importado.

É necessário se importar um certificado raiz para cada Autoridade Certificadora criada, caso contrário não será possível se autenticar usuários por meio dela.

O Campo **Pseudo-grupos** permite com que se defina grupos para usuários que se autenticarem através da autoridade certificadora, da mesma forma como se define grupos em um sistema operacional. Desta maneira, é possível se criar pseudo-grupos que representem todos os usuários de uma determinada empresa, departamento, cidade, etc. Após serem criados os pseudo-grupos eles podem ser associados a perfis de acesso da mesma forma com que se faz com grupos de autenticadores ou autenticadores token. Clicando com o botão direito podemos selecionar as seguintes opções:

- **Inserir:** Esta opção permite se incluir um novo pseudo-grupo.
- **Excluir**: Esta opção remove da lista o pseudo-grupo selecionado.
- **Editar:** Esta opção abre a janela de edição para o pseudo-grupo selecionado.

Ao se clicar no botão *Inserir* ou *Editar*, a seguinte janela será mostrada:

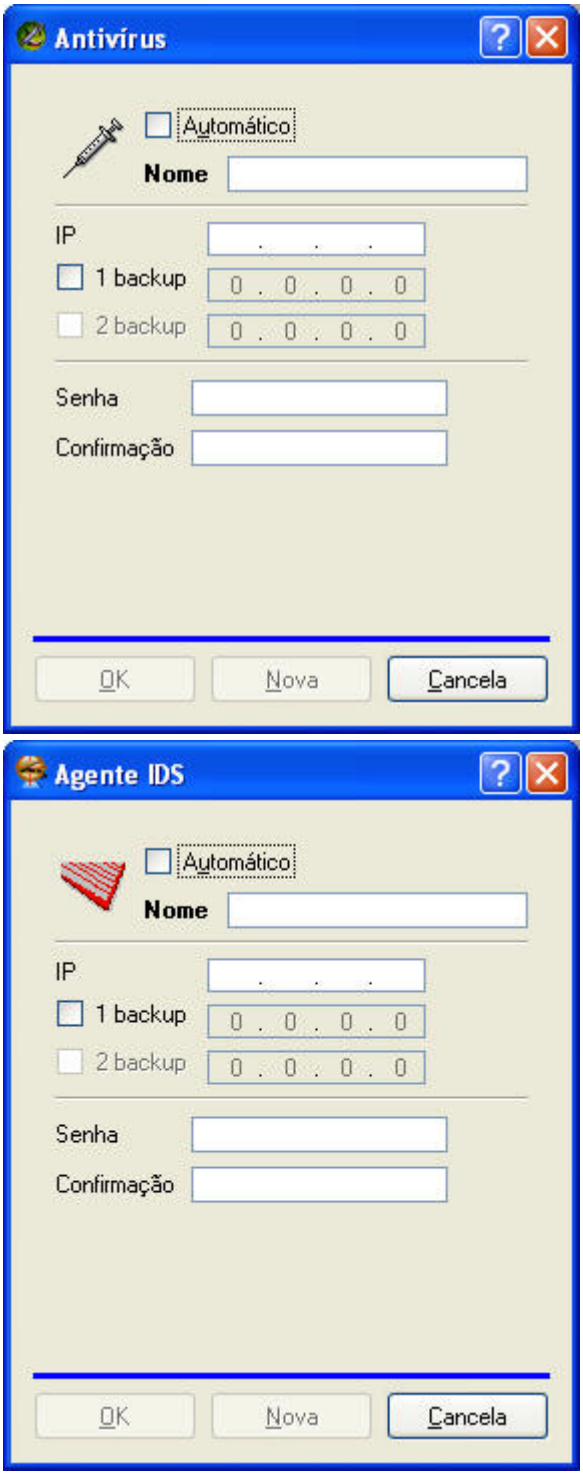


O único campo de preechimento obrigatório é o campo **Nome**, que indicará o nome pelo qual o pseudo-grupo será referenciado pelo firewall. Os demais campos representam dados que serão comparados com os dados presentes no certificado X509 de cada usuário autenticado. Caso um determinado campo esteja em branco então qualquer valor será aceito no campo correspondente do certificado, caso contrário apenas certificados que possuírem o campo igual ao valor informado serão considerados como parte do grupo.

O QUE SAO AS LETRAS ENTRE PARENTESES?
Domínio: Representa o nome da pessoa para a qual o certificado foi emitido
E-mail: Representa o e-mail da pessoa para a qual o certificado foi emitido
Empresa: Representa o nome da empresa onde trabalha a pessoa para a qual o certificado foi emitido
Departamento: Representa o departamento dentro da empresa onde trabalha a pessoa para a qual o certificado foi emitido
Cidade: Representa a cidade onde se localiza a empresa onde trabalha a pessoa para a qual o certificado foi emitido
Estado: Representa o estado onde se localiza a empresa onde trabalha a pessoa para a qual o certificado foi emitido
País: Representa o país onde se localiza a empresa onde trabalha a pessoa para a qual o certificado foi emitido

Para que um usuário autenticado através da autoridade certificadora seja considerado como membro de um pseudo-grupo, todos os campos de seu certificado X509 devem ser iguais aos valores dos campos correspondentes do pseudo-grupo. Campos em branco de um pseudo-grupo são ignorados na comparação e, portanto, quaisquer valores do certificado para estes campos serão aceitos.

- Para se cadastrar um agente externo do tipo **Agente IDS, Analisador de contexto**, **Anti-vírus** ou **Servidor de Log Remoto**, é necessário preencher os seguintes campos adicionais:



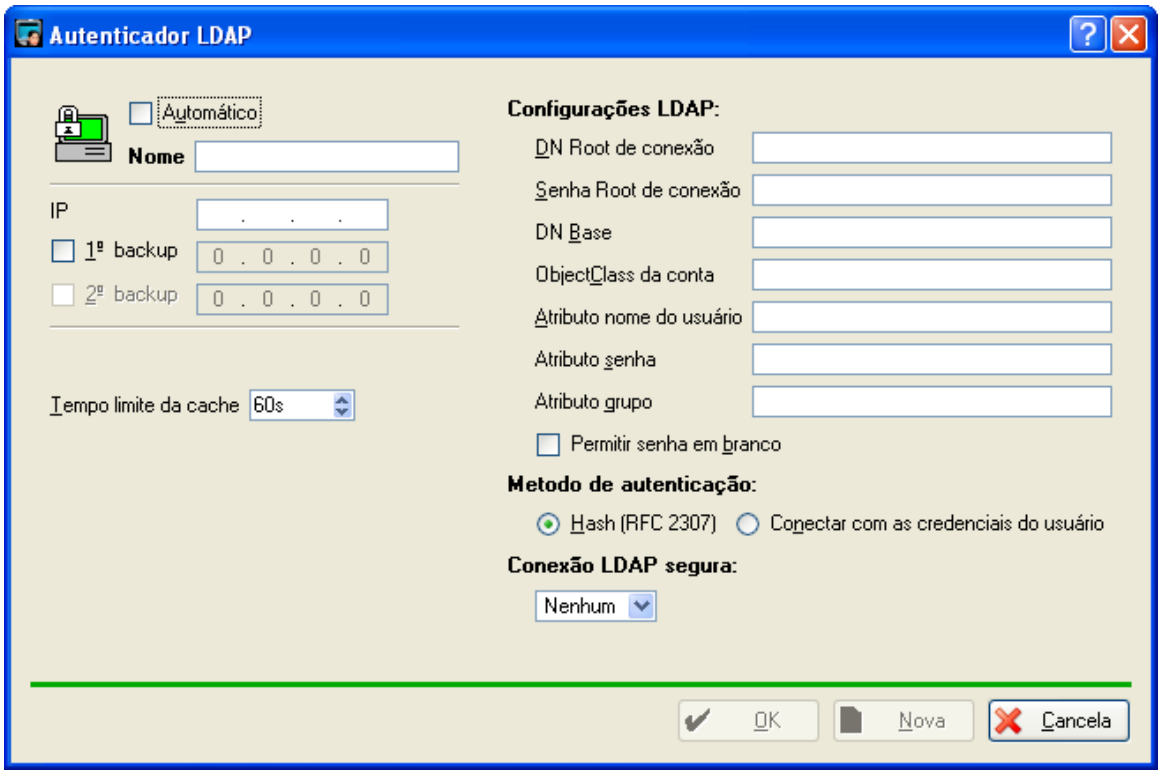
IP: É o endereço IP da máquina onde o agente está rodando.

Backup 1 e **Backup 2**: Estes campos permitem com que se especifique até dois endereços de outras máquinas que também estarão rodando o agente e que servirão como backup no caso de quedas da máquina principal.

Senha: É a senha utilizada para gerar as chaves de autenticação e criptografia usadas na comunicação com o agente. Esta senha deve ser igual à configurada no agente.

Confirmação: Este campo é utilizado apenas para se verificar se a senha foi digitada corretamente. Deve-se digitá-la exatamente como no campo *Senha*.

- Para se cadastrar um agente externo do tipo **Autenticador LDAP**, é necessário preencher os seguintes campos:



IP: É o endereço IP da máquina onde o agente está rodando.

Backup 1 e **Backup 2**: Estes campos permitem com que se especifique até dois endereços de outras máquinas que também estarão rodando o servidor LDAP e que servirão como backup no caso de quedas da máquina principal.

Tempo limite da cache: Todas as vezes que realiza uma autenticação com sucesso, o firewall mantém em memória os dados recebidos do usuário e do agente. Nas autenticações seguintes, o firewall possui todos os dados necessários e não mais precisa consultar o agente. Isso permite um grande ganho de performance.

Este parâmetro permite definir o tempo, em segundos, que o firewall deve manter as informações de autenticação em memória. Para maiores informações, veja o capítulo intitulado Trabalhando com proxies.

Configurações LDAP: Neste conjunto de campos deve-se especificar as configurações do servidor LDAP que será utilizado para a realização das autenticações. A descrição de cada campo pode ser vista a seguir:

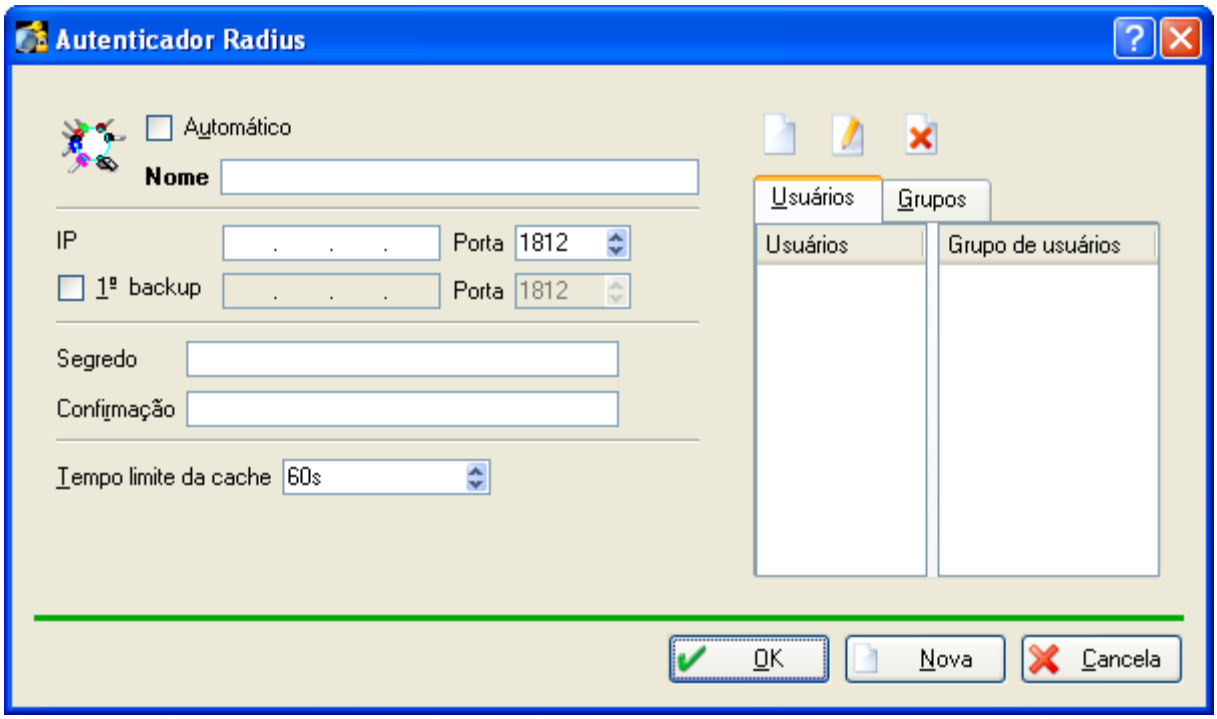
DN Root de conexão: DN do usuário utilizado pelo firewall para as consultas
Senha Root de conexão: a senha deste usuário
DN Base: DN para começar a busca
ObjectClass da Conta: valor de *objectclass* que identifica objetos de contas válidas
Atributo nome do usuário: o atributo onde se encontra o nome do usuário
Atributo senha: o atributo onde se encontra a senha do usuário
Atributo grupo: o atributo onde se encontra o grupo do usuário
Permitir senha em branco: permite senhas em branco para o usuário quando marcado

Método de Autenticação: Este campo especifica se o firewall deve buscar a senha ou se conectar na base LDAP com as credenciais do usuário para validá-lo.

Conexão LDAP segura: Este campo especifica se a conexão ao servidor LDAP será encriptada ou não. Ele consiste das seguintes opções:

- **SSL**: especifica que o firewall usará conexão encriptada via SSL
- **TLS**: especifica que o firewall usará conexão encriptada via TLS
- **Nenhuma**: especifica que o firewall não usará criptografia ao se conectar ao servidor LDAP

- Para se cadastrar um agente externo do tipo **Autenticador Radius**, é necessário preencher os seguintes campos adicionais:



IP: É o endereço IP da máquina onde o agente está rodando.

Porta: Número da porta onde o servidor RADIUS estará escutando as requisições de autenticação.

1º Backup: Este campo permite com que se especifique outra máquina que também estará rodando o servidor RADIUS e que servirá como backup no caso de queda da máquina principal.

Segredo: É o segredo compartilhado utilizado no servidor RADIUS.

Confirmação: Este campo é utilizado apenas para se verificar se o segredo foi digitado corretamente. Deve-se digitá-lo exatamente como no campo *Segredo*.

Tempo limite de uso da cache: Todas as vezes que realiza uma autenticação com sucesso, o firewall mantém em memória os dados recebidos do usuário e do agente. Nas autenticações seguintes, o firewall possui todos os dados necessários e não mais precisa consultar o agente. Isso permite um grande ganho de performance.

Este parâmetro permite definir o tempo, em segundos, que o firewall deve manter as informações de autenticação em memória. Para maiores informações, veja o capítulo intitulado Trabalhando com proxies.

Usuários: Este campo serve para que se possa cadastrar e posteriormente associar usuários específicos RADIUS com perfis de acesso do firewall, uma vez que com este protocolo não é possível para o firewall conseguir a lista completa de usuários. Somente é necessário se realizar o cadastramento dos usuários que se deseje associar com perfis específicos.

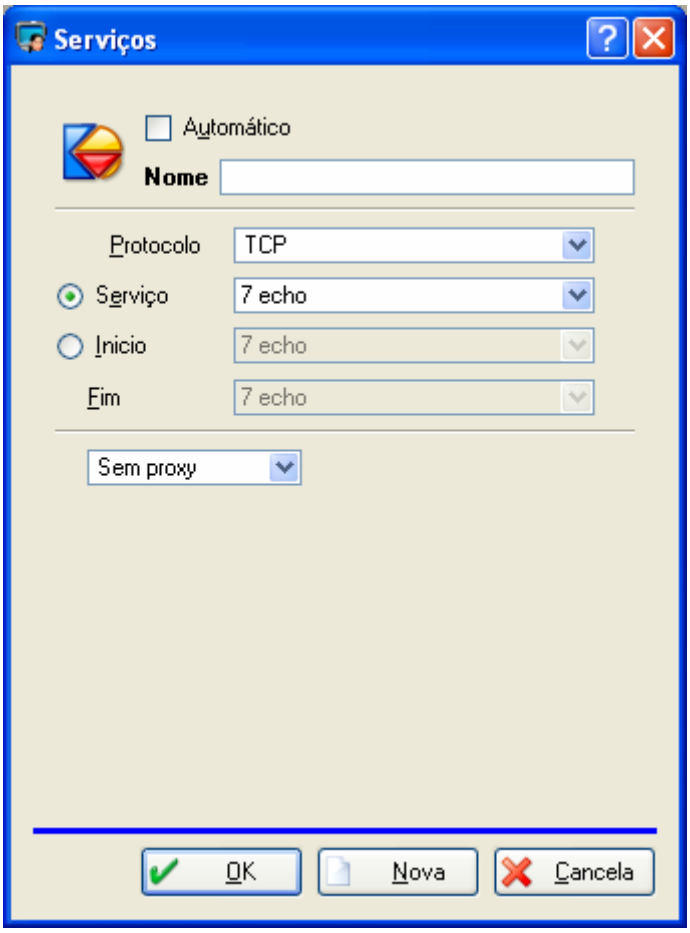
Grupos: Este campo serve para que se possa cadastrar e posteriormente associar grupos específicos RADIUS com perfis de acesso do firewall, uma vez que com este protocolo não é possível para o firewall conseguir a lista completa de grupos. Somente é necessário se realizar o cadastramento dos grupos que se deseje associar com perfis específicos.

Existe um grupo chamado de **RADIUS USERS**, gerado automaticamente pelo firewall que pode ser utilizado para a associação de usuários RADIUS com um perfil de acesso específico. Todos os usuários autenticados em um determinado servidor RADIUS são considerados como pertencentes a este grupo. Desta forma, caso se deseje utilizar um único perfil de acesso para todos os usuários, não é necessário o cadastramento de nenhum usuário e/ou grupo.

Após todos os campos estarem preenchidos, deve-se clicar no botão **OK** para realizar a inclusão ou alteração do agente externo. Para cancelar as alterações realizadas ou a inclusão, deve-se pressionar o botão **Cancelar**.

Para facilitar a inclusão de vários agentes seguidamente, existe um botão chamado **Nova** (que não estará habilitado durante uma edição). Ao ser clicado, este botão fará com que o agente cujos dados foram preenchidos seja incluído e a janela de inclusão de agentes mantida aberta, pronta para uma nova inclusão. Desta forma, é possível se cadastrar rapidamente um grande número de agentes.

Incluindo / editando serviços



Para se cadastrar uma entidade do tipo serviço, é necessário preencher os seguintes campos:

Nome: É o nome através do qual o serviço será referenciado daqui em diante pelo firewall. É possível se especificar este nome manualmente ou deixar que ele seja atribuído automaticamente. A opção **Automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Letras maiúsculas e minúsculas são consideradas diferentes nos nomes das entidades. Desta forma, é possível a existência de várias entidades compostas de nomes com as mesmas letras, porém com combinações distintas de maiúsculas e minúsculas. As entidades **Aker**, **AKER** e **aker** são, portanto, consideradas diferentes.

Ícone: É o ícone que aparecerá associado ao serviço em todas as referências. Para alterá-lo, basta clicar sobre o desenho do ícone atual. O firewall então mostrará uma lista com todos os possíveis ícones para representar serviços. Para escolher entre eles basta clicar no ícone desejado e no botão **OK**. Caso não se deseje alterá-lo após ver a lista, basta clicar no botão **Cancelar**.

Protocolo: É o protocolo associado ao serviço.(TCP, UDP, ICMP ou OUTROS)

Serviço: É o número que identifica o serviço. No caso dos protocolos TCP e UDP, este número é a porta destino. No caso de ICMP é o tipo de serviço e no caso de outros protocolos é o número do protocolo. Para cada protocolo, o firewall possui uma lista dos valores mais comuns associados a ele, de modo a facilitar a criação do serviço. Entretanto, é possível colocar valores que não façam parte da lista, simplesmente digitando-os neste campo.

Caso se deseje especificar uma faixa de valores, ao invés de um único valor, basta-se clicar no botão ao lado dos nomes **De** e **Para** e especificar o menor valor da faixa em **De** e o maior em **Para**. Todos os valores compreendidos entre estes dois, inclusive, serão considerados como fazendo parte do serviço.

Proxy: Este campo só se encontra habilitado para os protocolos TCP e UDP e permite especificar se a conexão que se enquadrar neste serviço será automaticamente desviada para um dos proxies transparentes do Firewall Aker ou não. O valor padrão é **Sem Proxy**, que significa que a conexão não deve ser desviada para nenhum proxy. Quando o protocolo TCP está selecionado, as outras opções são **Proxy SMTP**, **Proxy Telnet**, **Proxy FTP, Proxy do usuário, Proxy HTTP** e **Proxy POP3** que desviam para os proxies SMTP, Telnet, FTP, proxies criados pelo usuário, HTTP e POP3, respectivamente. Quando o protocolo UDP está selecionado, as outras opções são **Proxy RPC**, que desvia para o proxy RPC, e **Proxy do Usuário**.

O serviço Telnet está associado à porta 23, o SMTP à porta 25, o FTP à porta 21, o HTTP à porta 80 e o POP3 à porta 110. É possível se especificar que conexões de quaisquer outras portas sejam desviadas para um destes proxies, entretanto, isto não é o comportamento padrão e não deve ser feito a não ser que se tenha conhecimento de todas as possíveis implicações.

Caso se tenha especificado que a conexão deve ser desviada para um proxy, pode ser necessário se definir os parâmetros do contexto que será utilizado pelo proxy para este serviço. Caso isso seja necessário, no momento em que o proxy for selecionado, a janela será expandida para mostrar os parâmetros adicionais que devem ser configurados.

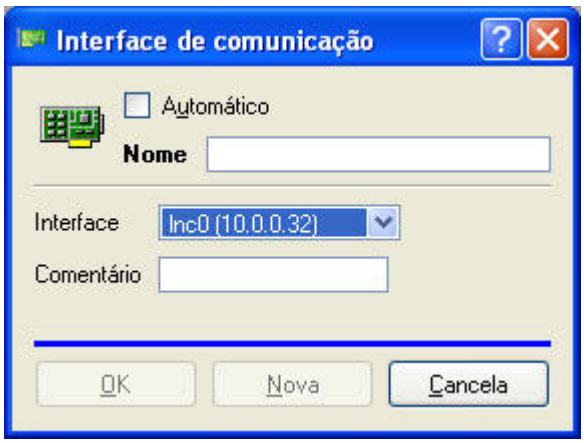
A explicação dos parâmetros de cada um dos contextos dos proxies padrão se encontra nos capítulos intitulados Configurando o proxy SMTP, Configurando o proxy Telnet, Configurando o proxy FTP, Configurando o proxy POP3 e Configurando o Proxy RPC. O proxy HTTP não tem parâmetros configuráveis e suas configurações são descritas no capítulo Configurando o proxy WWW. Para maiores informações sobre proxies transparentes e contextos, veja o capítulo intitulado Trabalhando com proxies. Proxies definidos pelo usuário somente são úteis para desenvolvedores e sua descrição não será abordada aqui.

Após todos os campos estarem preenchidos, deve-se clicar no botão **OK** para realizar a inclusão ou alteração do serviço. Para cancelar as alterações realizadas ou a inclusão, deve-se pressionar o botão **Cancelar** .

Para facilitar a inclusão de vários serviços seguidamente, existe um botão chamado **Nova** (que não estará habilitado durante uma edição). Ao ser clicado, este botão fará com que o serviço cujos dados foram preenchidos seja incluído e a janela de inclusão de

serviços mantida aberta, pronta para uma nova inclusão. Desta forma, é possível se cadastrar rapidamente um grande número de serviços.

Incluindo / editando interfaces



Para se cadastrar uma entidade do tipo interface, é necessário preencher os seguintes campos:

Nome: É o nome através do qual a interface será referenciada daqui em diante pelo firewall. É possível se especificar este nome manualmente ou deixar que o ele seja atribuído automaticamente. A opção **Automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Letras maiúsculas e minúsculas são consideradas diferentes nos nomes das entidades. Desta forma, é possível a existência de várias entidades compostas de nomes com as mesmas letras, porém com combinações distintas de maiúsculas e minúsculas. As entidades **Aker**, **AKER** e **aker** são, portanto, consideradas diferentes.

Ícone: É o ícone que aparecerá associado à interface em todas as referências. Para alterá-lo, basta clicar sobre o desenho do ícone atual. O firewall então mostrará uma lista com todos os possíveis ícones para representar interfaces. Para escolher entre eles basta clicar no ícone desejado e no botão **OK**. Caso não se deseje alterá-lo após ver a lista, basta clicar no botão **Cancelar**.

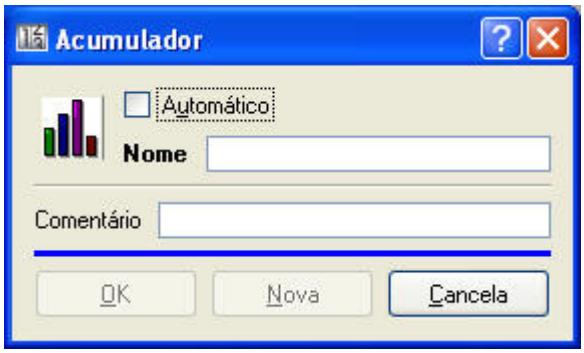
Interface: É o nome do adaptador de rede que será associado à entidade interface. Será mostrada automaticamente uma lista com todos os adaptadores de rede configurados no firewall e o endereço IP de cada um, se existir.

Comentário: É um campo texto livre, usado apenas para fins de documentação.
Após todos os campos estarem preenchidos, deve-se clicar no botão **OK** para realizar a inclusão ou alteração da interface. Para cancelar as alterações realizadas ou a inclusão, deve-se pressionar o botão **Cancelar** .

Para facilitar a inclusão de várias interfaces seguidamente, existe um botão chamado **Nova** (que não estará habilitado durante uma edição). Ao ser clicado, este botão fará com que a interface cujos dados foram preenchidos seja incluída e a janela de inclusão de interfaces mantida aberta, pronta para uma nova inclusão. Desta forma, é possível se cadastrar rapidamente um grande número de interfaces.

Incluindo / editando acumuladores

Acumuladores são entidades usadas em regras de filtragem com o objetivo de coletar estatísticas sobre o tráfego de rede. Um mesmo acumulador pode ser utilizado em várias regras de filtragem e o tráfego que se encaixar em cada uma destas regras é sumarizado pelo acumulador. Seu uso está descrito melhor nos capítulos O Filtro de Estados e Visualizando estatísticas.



Para se cadastrar uma entidade do tipo acumulador, é necessário preencher os seguintes campos:
Nome: É o nome através do qual o acumulador será referenciado daqui em diante pelo firewall. É possível se especificar este nome manualmente ou deixar que o ele seja atribuído automaticamente. A opção **Automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Letras maiúsculas e minúsculas são consideradas diferentes nos nomes das entidades. Desta forma, é possível a existência de várias entidades compostas de nomes com as mesmas letras, porém com combinações distintas de maiúsculas e minúsculas. As entidades **Aker**, **AKER** e **aker** são, portanto, consideradas diferentes.

Ícone: É o ícone que aparecerá associado ao acumulador em todas as referências. Para alterá-lo, basta clicar sobre o desenho do ícone atual. O firewall então mostrará uma lista com todos os possíveis ícones para representar interfaces. Para escolher entre eles basta clicar no ícone desejado e no botão **OK**. Caso não se deseje alterá-lo após ver a lista, basta clicar no botão **Cancelar**.

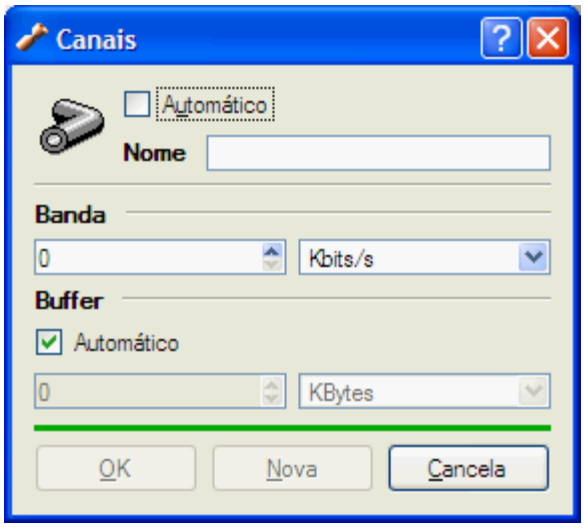
Comentário: É um campo texto livre, usado apenas para fins de documentação.

Após todos os campos estarem preenchidos, deve-se clicar no botão **OK** para realizar a inclusão ou alteração do acumulador. Para cancelar as alterações realizadas ou a inclusão, deve-se pressionar o botão **Cancelar** .

Para facilitar a inclusão de vários acumuladores seguidamente, existe um botão chamado **Nova** (que não estará habilitado durante uma edição). Ao ser clicado, este botão fará com que o acumulador cujos dados foram preenchidos seja incluído e a janela de inclusão de acumuladores mantida aberta, pronta para uma nova inclusão. Desta forma, é possível se cadastrar rapidamente um grande número de acumuladores.

Incluindo / editando Canais

Canais são entidades usadas em regras de filtragem com o objetivo de limitar a banda de determinados serviços, máquinas, redes e/ou usuários. Seu uso está descrito no capítulo O Filtro de Estados.



Para se cadastrar uma entidade do tipo Canal, é necessário preencher os seguintes campos:
Nome: É o nome através do qual o Canal será referenciado daqui em diante pelo firewall. É possível se especificar este nome manualmente ou deixar que o ele seja atribuído automaticamente. A opção **Nome automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Letras maiúsculas e minúsculas são consideradas diferentes nos nomes das entidades. Desta forma, é possível a existência de várias entidades compostas de nomes com as mesmas letras, porém com combinações distintas de maiúsculas e minúsculas. As entidades **Aker**, **AKER** e **aker** são, portanto, consideradas diferentes.

Ícone: É o ícone que aparecerá associado ao Canal em todas as referências. Para alterá-lo, basta clicar sobre o desenho do ícone atual. O firewall então mostrará uma lista com todos os possíveis ícones para representar interfaces. Para escolher entre eles basta clicar no ícone desejado e no botão **OK**. Caso não se deseje alterá-lo após ver a lista, basta clicar no botão **Cancelar**.

Banda: É um campo texto usado para designar a largura de banda (velocidade máxima de transmissão em bits por segundo) deste Canal. Esta banda será compartilhada entre

todas as conexões que usarem este Canal. Deve ser escolhida a unidade de medida mais conveniente.

Buffer: É um campo texto usado para designar o tamanho do buffer (espaço temporário de dados utilizado para armazenar pacotes que serão transmitidos) utilizado por este Canal. Deve ser escolhido a unidade de medida. É possível se especificar este tamanho manualmente ou deixar que o ele seja atribuído automaticamente. A opção **Automático** permite escolher entre estes dois modos de operação: caso ela esteja marcada, a atribuição será automática, caso contrário, manual.

Após todos os campos estarem preenchidos, deve-se clicar no botão **OK** para realizar a inclusão ou alteração do Canal. Para cancelar as alterações realizadas ou a inclusão, deve-se pressionar o botão **Cancelar** .

Para facilitar a inclusão de vários Canais seguidamente, existe um botão chamado **Nova** (que não estará habilitado durante uma edição). Ao ser clicado, este botão fará com que o Canal cujos dados foram preenchidos seja incluído e a janela de inclusão de Canais mantida aberta, pronta para uma nova inclusão. Desta forma, é possível se cadastrar rapidamente um grande número de Canais.

5-3 Utilizando a interface texto

A utilização da interface texto na configuração das entidades é bastante simples e possui praticamente todos os recursos da interface gráfica. As únicas opções não disponíveis são a criação de serviços que utilizem proxies transparentes e a edição de pseudo-grupos de uma autoridade certificadora. É importante comentar, entretanto, que na interface texto os agentes externos são mostrados e criados diretamente pelo seu sub-tipo.
Localização do programa : `/etc/firewall/fwent`

Sintaxe:

```
Uso: fwent ajuda
     fwent mostra
     fwent remove <nome>
     fwent inclui maquina <nome> <IP>
     fwent inclui rede <nome> <IP> <mascara>
     fwent inclui conjunto <nome> [<entidade1> [<entidade2>] ...]
     fwent inclui autenticador <nome> <IP1> [<IP2>] [<IP3>] <senha>
<t. cache>
     fwent inclui token <nome> <IP1> [<IP2>] [<IP3>] <senha> <t.
cache>
     fwent inclui ldap <nome> <IP1> [<IP2>] [<IP3>] <root_dn>
<root_pwd>
                        <base_dn> <act_class> <usr_attr> <grp_attr>
                        < <pwd_attr>|<-bind> > < <-ssl>|<-tls>|<-
nenhuma> >
                        < <-no_pwd>|<-pwd> > <t.cache>
     fwent inclui radius <nome> <IP1> <porta1> [ <IP2> <porta2> ]
<senha> <t.cache>
     fwent inclui ids <nome> <IP1> [<IP2>] [<IP3>] <senha>
     fwent inclui anti-virus <nome> <IP1> [<IP2>] [<IP3>] <senha>
     fwent inclui analisador-url <nome> <IP1> [<IP2>] [<IP3>] <senha>
     fwent inclui ca <nome> <Arquivo com certificado root> <URL com
CRLs>
```

```
     fwent inclui servico <nome> [TCP | UDP | ICMP | OUTRO]
<valor>[..<valor>]
     fwent inclui interface <nome> <dispositivo> [<comentario>]
     fwent inclui pipe <nome> <banda em Kbits/s> [<tamanho da fila>
<bytes|pacts>]
     fwent inclui acumulador <nome> [<comentario>]
     fwent inclui log_remoto <nome> <IP> [IP] [IP] <senha>
```

Ajuda do programa :

```
fwent - Interface texto para configuracao das entidades
Uso: fwent ajuda
     fwent mostra
     fwent remove <nome>
     fwent inclui maquina <nome> <IP>
     fwent inclui rede <nome> <IP> <mascara>
     fwent inclui conjunto <nome> [<entidade1> [<entidade2>] ...]
     fwent inclui autenticador <nome> <IP1> [<IP2>] [<IP3>] <senha>
<t. cache>
     fwent inclui token <nome> <IP1> [<IP2>] [<IP3>] <senha> <t.
cache>
     fwent inclui ldap <nome> <IP1> [<IP2>] [<IP3>] <root_dn>
<root_pwd>
                       <base_dn> <act_class> <usr_attr> <grp_attr>
                       < <pwd_attr>|<-bind> > < <-ssl>|<-tls>|<-
nenhuma> >
                       < <-no_pwd>|<-pwd> > <t.cache>
     fwent inclui radius <nome> <IP1> <porta1> [ <IP2> <porta2> ]
<senha> <t.cache>
     fwent inclui ids <nome> <IP1> [<IP2>] [<IP3>] <senha>
     fwent inclui anti-virus <nome> <IP1> [<IP2>] [<IP3>] <senha>
     fwent inclui analisador-url <nome> <IP1> [<IP2>] [<IP3>] <senha>
     fwent inclui ca <nome> <Arquivo com certificado root> <URL com
CRLs>
     fwent inclui servico <nome> [TCP | UDP | ICMP | OUTRO]
<valor>[..<valor>]
     fwent inclui interface <nome> <dispositivo> [<comentario>]
     fwent inclui pipe <nome> <banda em Kbits/s> [<tamanho da fila>
<bytes|pacts>]
     fwent inclui acumulador <nome> [<comentario>]
     fwent inclui log_remoto <nome> <IP> [IP] [IP] <senha>
     mostra   = mostra todas as entidades configuradas no sistema
     inclui   = inclui uma nova nova entidade
     remove   = remove uma entidade existente
     ajuda    = mostra esta mensagem
Para remove / inclui temos:
     nome     = nome da entidade a ser criada ou removida
Para inclui temos:
     IP       = endereco IP da maquina ou da rede
     mascara  = mascara da rede
     entidade = nome das entidades a serem acrescentadas no conjunto
                (OBS: Somente podem fazer parte de um conjunto
entidades
                 do tipo maquina ou rede)
     senha    = senha de acesso
     t. cache = tempo em segundos de permanencia de uma entrada no
cache de
                autenticacao
     TCP      = servico utiliza protocolo TCP
     UDP      = servico utiliza protocolo UDP
     ICMP     = servico utiliza protocolo ICMP
     OUTRO    = servico utiliza protocolo diferente dos acima citados
     valor    = Numero que identica o servico. Para os protocolos TCP
```

```
e UDP,
                e' o valor da porta associada ao servico. No caso de
ICMP, e' o
                tipo de servico e no caso de outros protocolos o
numero do
                proprio protocolo. Pode-se especificar uma faixa
atraves da
                notacao valor1..valor2, que significa a faixa de
valores
                compreendida entre o valor1 e o valor2 (inclusive).
Para inclui ldap temos:
       root_dn  = DN do usuario utilizado pelo firewall para as
consultas
       root_pwd = a senha deste usuario
       base_dn  = DN para comecar a busca
       act_class= valor de objectclass que identifica objetos de
contas validas
       usr_attr = o atributo onde se encontra o nome do usuario
       grp_addr = o atributo onde se encontra o grupo do usuario
       pwd_addr = o atributo onde se encontra a senha do usuario
       -bind    = nao tenta buscar a senha, em vez disso tenta
conectar na base
                  LDAP com as credenciais do usuario para valida-lo
       -ssl     = usar conexao encriptada via ssl
       -tls     = usar conexao encriptada via tls
       -nenhuma = nao usar conexao encriptada
       -no_pwd  = permite senhas em branco para o usuario
       -pwd     = nao permite senhas em branco para o usuario
```

Exemplo 1 : (visualizando as entidades definidas no sistema)

```
#fwent mostra

Maquinas:
---------
cache                     10.4.1.12
firewall                  10.4.1.11

Redes:
------
AKER                      10.4.1.0        255.255.255.0
Internet                  0.0.0.0         0.0.0.0

Conjuntos:
----------
Maquinas Internas         cache                     firewall

Autenticadores:
---------------
Autenticador NT           10.0.0.1
10.0.0.2                        600
Unix                      192.168.0.1     192.168.0.2
192.168.0.3      600

Autenticadores do tipo token:
-----------------------------
Autenticador token        10.0.0.1
10.0.0.2                        600

Agentes IDS:
------------
Agente IDS                 10.10.0.1
```

```
Anti-Virus:
-----------
Anti-virus local            127.0.0.1

Servicos:
---------
echo reply                  ICMP  8
echo request                ICMP  0
ftp                         TCP   21
snmp                        UDP   161
telnet                      TCP   23

Interfaces:
-----------
Interface Externa           xl0
Interface Interna           de0
```

Exemplo 2: (cadastrando uma entidade do tipo máquina)

```
#/etc/firewall/fwent inclui maquina Servidor_1 10.4.1.4
Entidade incluida
```

Exemplo 3: (cadastrando uma entidade do tipo rede)

```
#/etc/firewall/fwent inclui rede Rede_1 10.4.0.0 255.255.0.0
Entidade incluida
```

Exemplo 4: (cadastrando uma entidade do tipo serviço)

```
#/etc/firewall/fwent inclui servico DNS UDP 53
Entidade incluida
```

Exemplo 5: (cadastrando uma entidade do tipo autenticador)

```
#/etc/firewall/fwent inclui autenticador "Autenticador Unix" 10.4.2.2
senha_123 900
Entidade incluida
```

O uso de "" ao redor do nome da entidade é obrigatório quando se inclui ou remove entidades cujo nome contém espaços

Exemplo 6: (incluindo uma entidade do tipo conjunto, cujos membros são as máquinas cache e firewall, previamente definidas)

```
#/etc/firewall/fwent inclui conjunto "Conjunto de teste" cache
firewall
Entidade incluida
```

Exemplo 7: (incluindo uma entidade do tipo interface, sem especificar um comentário)

```
#/etc/firewall/fwent inclui interface "Interface DMZ" fxp0
Entidade incluida
```

Exemplo 8: (incluindo uma entidade do tipo autenticador token, utilizando uma máquina primária e uma secundária, como backup)

```
#/etc/firewall/fwent inclui token "Autenticador token" 10.0.0.1
10.0.0.2 senha 600
Entidade incluida
```

Exemplo 9: (removendo uma entidade)

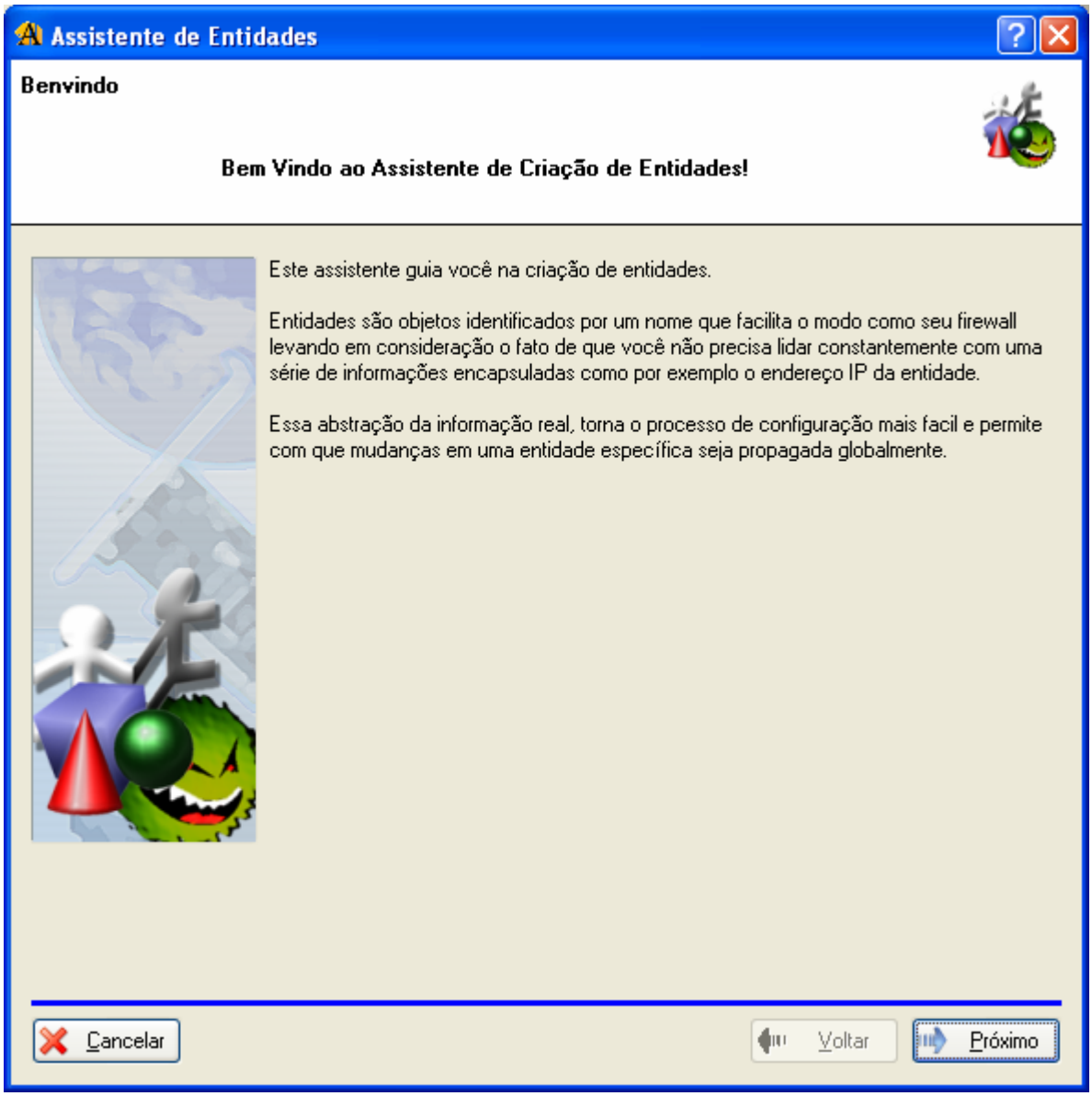
```
#/etc/firewall/fwent remove "Autenticador Unix"
Entidade removida
```

5-4 Utilizando o Assistente de Entidades

O assistente de criação de entidades pode ser invocado clicando-se no ícone , localizado na parte inferior da janela de entidades. Sua idéia é simplificar a tarefa de criação das entidades e pode ser utilizado sempre que desejado. Ele consiste de várias janelas mostradas em série, a depender do tipo de entidade a ser criada.

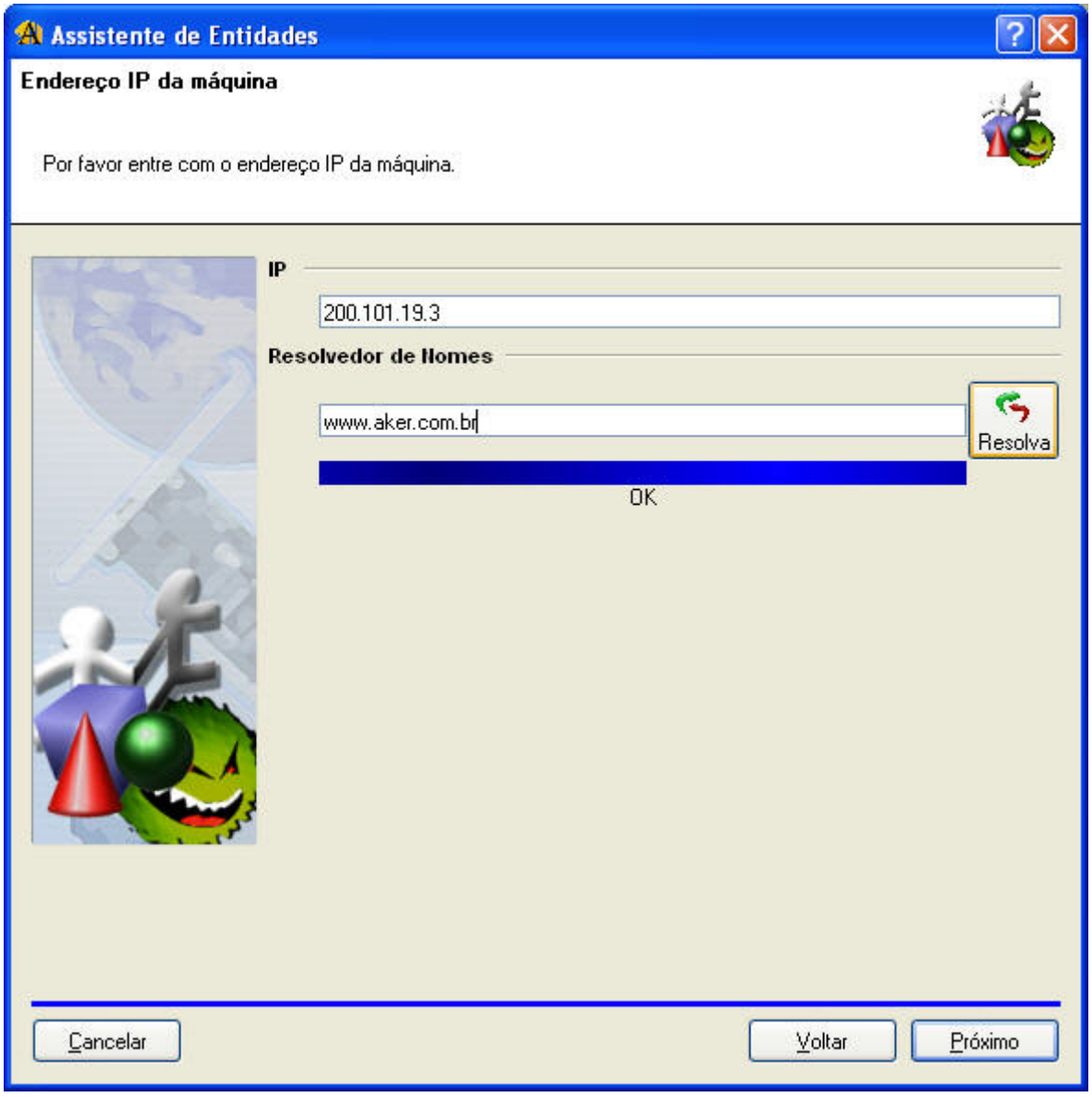
Seu uso é extremamente simples e o exemplificaremos para a criação de uma entidade do tipo máquina:

1 - A primeira janela mostrada é uma breve explicação dos procedimentos a serem realizados:

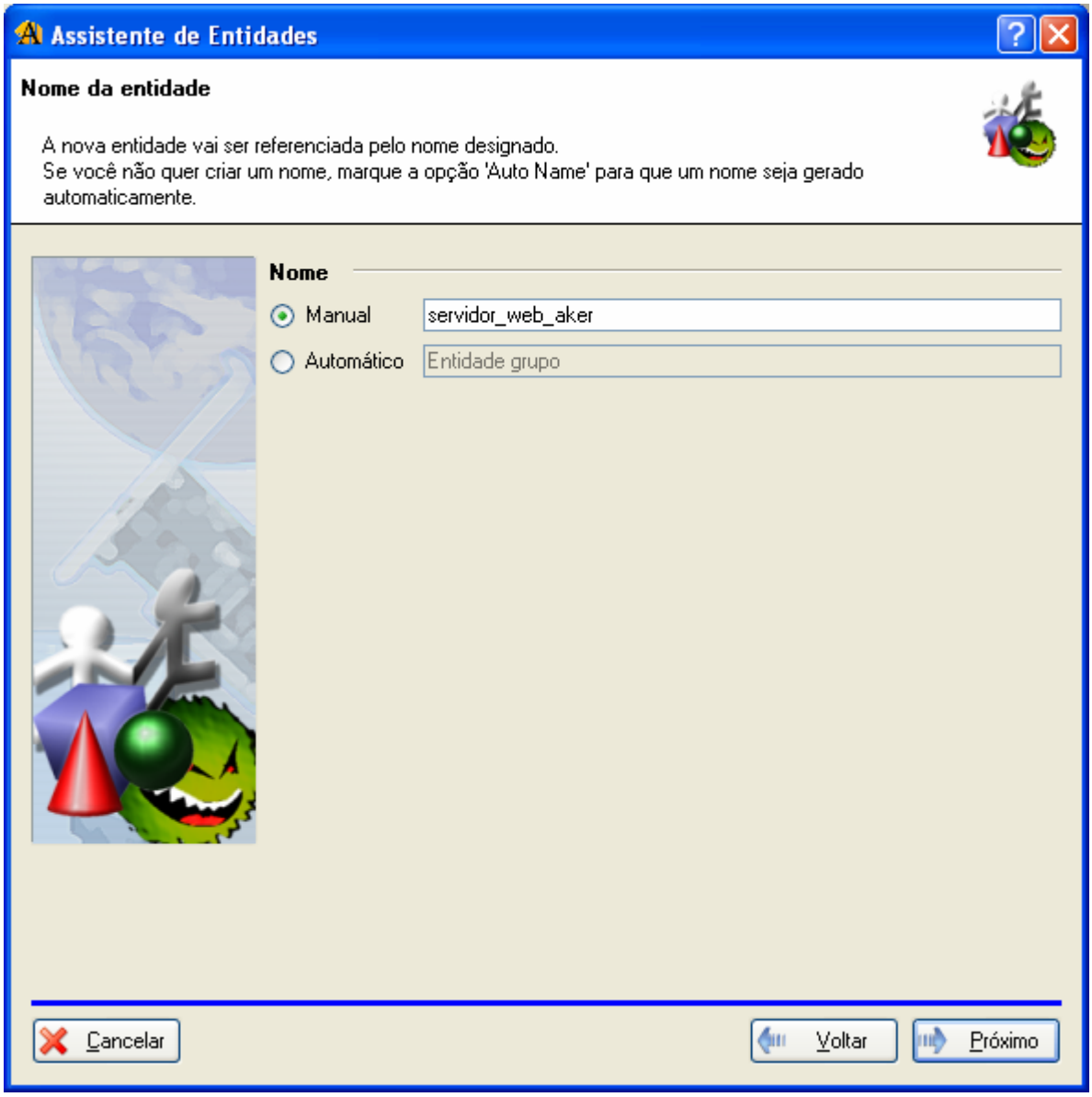

Assistente de Entidades
Benvindo
Bem Vindo ao Assistente de Criação de Entidades!
Este assistente guia você na criação de entidades.
Entidades são objetos identificados por um nome que facilita o modo como seu firewall levando em consideração o fato de que você não precisa lidar constantemente com uma série de informações encapsuladas como por exemplo o endereço IP da entidade.
Essa abstração da informação real, torna o processo de configuração mais facil e permite com que mudanças em uma entidade específica seja propagada globalmente.
Cancelar
Voltar
Próximo

2 - Na segunda janela se deve escolher o tipo de entidade a ser cadastrada:

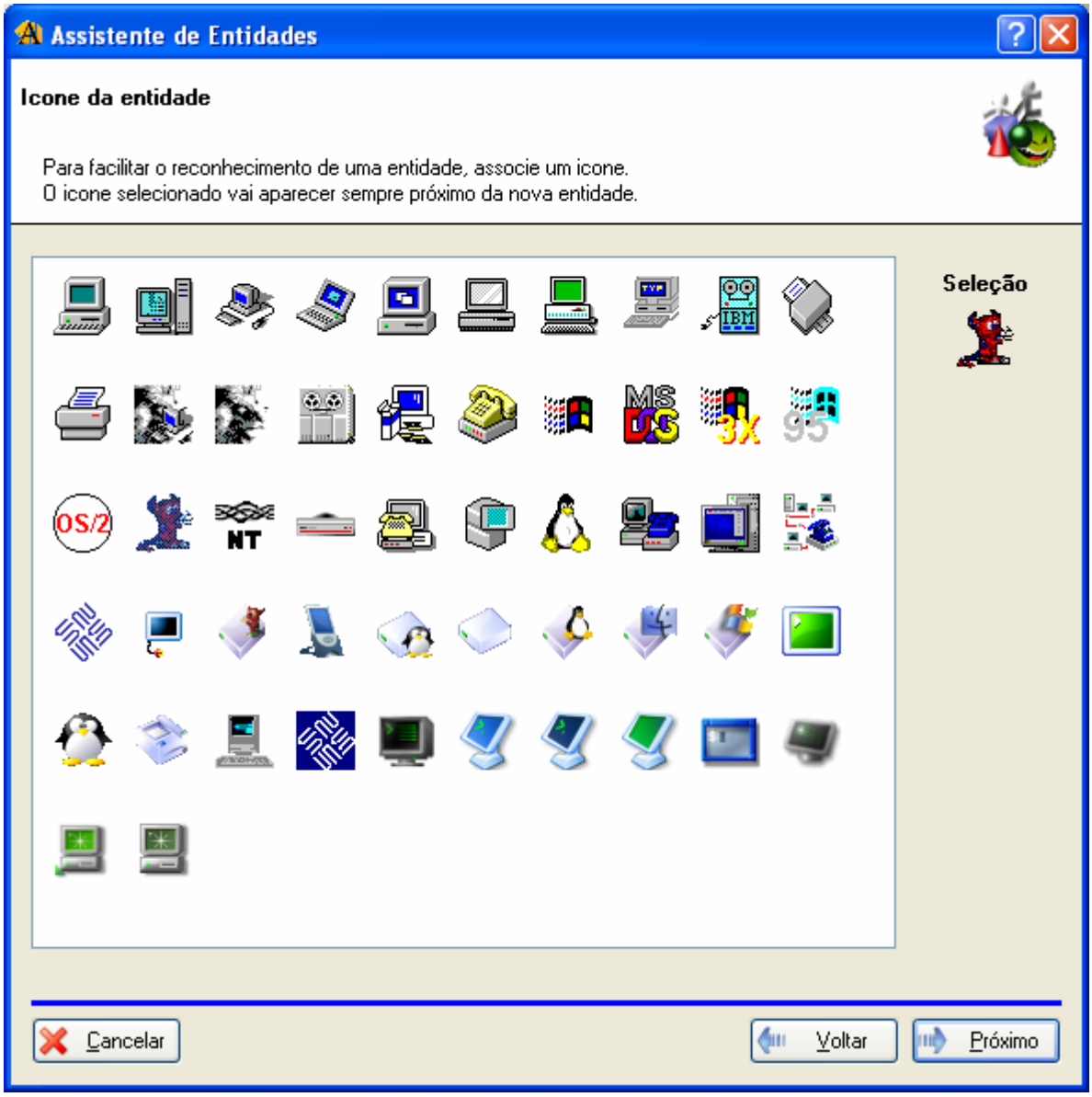
3 - No caso do cadastro de uma máquina, nesta janela se deve especificar o endereço IP da mesma. É possível se colocar o nome da máquina e clicar no botão *Resolva* para obter o endereço IP correspondente.



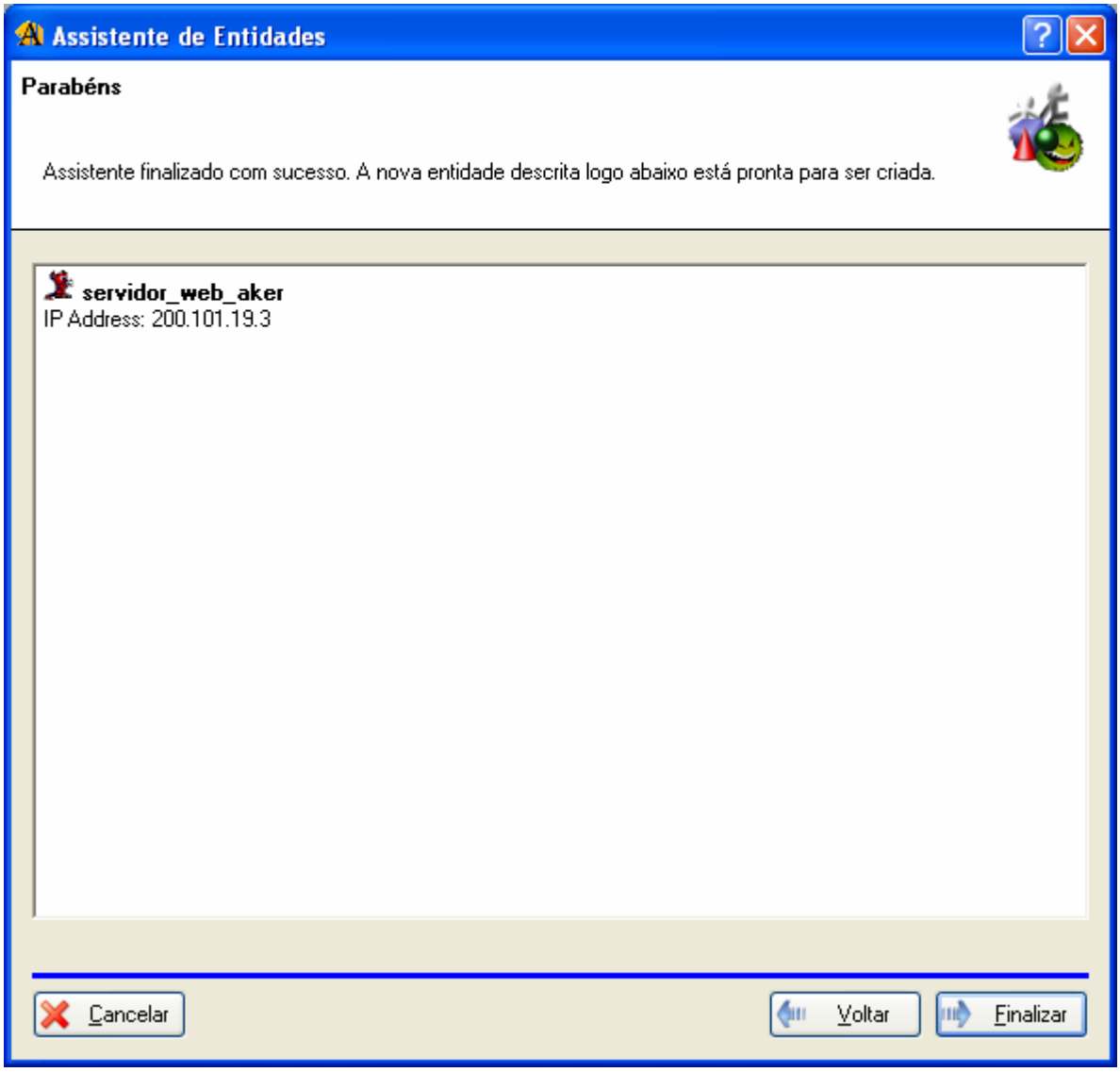
4 - Atribuição do nome da entidade. Pode-se escolher o nome ou usar a atribuição automática.



5 - Escolha do ícone da entidade. Clique em um dos ícones que aparecem na janela. Observe que o ícone selecionado irá aparecer à direita da janela.



6 - Finalização do cadastramento. Será mostrado um resumo com os dados da entidade. Basta-se clicar no botão *Finalizar* para cadastrar a entidade.


Assistente de Entidades
Parabéns
Assistente finalizado com sucesso. A nova entidade descrita logo abaixo está pronta para ser criada.
servidor_web_aker
IP Address: 200.101.19.3
Cancelar
Voltar
Finalizar

6-0 O Filtro de Estados

Mostraremos aqui como configurar as regras que propiciarão a aceitação ou não de conexões pelo firewall. Este módulo é o coração do sistema e é onde normalmente se gasta o maior tempo de configuração.

6-1 Planejando a instalação

O que é um filtro de pacotes ?

Um filtro de pacotes é o módulo que irá decidir se um determinado pacote poderá passar através do firewall ou não. Deixar um pacote passar implica em aceitar um determinado serviço. Bloquear um pacote significa impedir que este serviço seja utilizado.

Para decidir a ação a ser tomada para cada pacote que chega ao firewall, o filtro de pacotes possui um conjunto de regras configurado pelo administrador do sistema. Para cada pacote que chega, o filtro de pacotes percorre este conjunto de regras, na ordem em que foi criado, verificando se este se encaixa em alguma das regras. Se ele se encaixar em uma regra então a ação definida para ela será executada. Caso o filtro termine a pesquisa de todas as regras e o pacote não se encaixar em nenhuma então a ação padrão será executada.

O que é o filtro de estados do Firewall Aker ?

Um filtro tradicional de pacotes baseia suas ações exclusivamente no conjunto de regras configurado pelo administrador. Para cada pacote que poderá passar pelo filtro, o administrador tem que configurar uma regra que possibilite sua aceitação. Em alguns casos isto é simples, mas em outros isto não é possível de ser feito ou pelo menos não é possível de se fazer com a segurança e flexibilidade necessárias.

O filtro de pacotes do Firewall Aker é chamado de filtro de estados na medida em que armazena informações do estado de todas as conexões que estão fluindo através dele e usa estas informações em conjunto com as regras definidas pelo administrador na hora de tomar a decisão de permitir ou não a passagem de um determinado pacote. Além disso, diferentemente de um filtro de pacotes que baseia suas decisões apenas nos dados contidos no cabeçalho do pacote, o filtro de estados examina dados de todas as camadas e utiliza todos estes dados ao tomar uma decisão.

Vamos analisar como isso permite a solução de diversos problemas apresentados pelos filtros de pacotes tradicionais.

O problema do protocolo UDP:

Para usar um serviço UDP, a máquina cliente inicialmente escolhe um número de porta (que é variável cada vez que o serviço for utilizado) e envia um pacote para a porta da máquina servidora correspondente ao serviço (esta porta na máquina servidora é fixa). A máquina servidora, ao receber a requisição, responde com um ou mais pacotes para a

porta da máquina cliente. Para que a comunicação seja efetiva, é necessário que o firewall permita a passagem dos pacotes de solicitação do serviço e de resposta. O problema é que o protocolo UDP é um protocolo não orientado à conexão, isto significa que se um determinado pacote for observado isoladamente, fora de um contexto, não se pode saber se ele é uma requisição ou uma resposta de um serviço.

Nos filtros de pacotes tradicionais, como o administrador não pode saber de antemão qual porta será escolhida pela máquina cliente para acessar um determinado serviço, ele pode ou bloquear todo o tráfego UDP ou permitir a passagem de pacotes para todas as possíveis portas. Ambas abordagens possuem problemas óbvios.

O Firewall Aker possui a capacidade de se adaptar dinamicamente ao tráfego de modo a resolver problemas deste tipo: todas as vezes que um pacote UDP é aceito por uma das regras configurada pelo administrador, é adicionada uma entrada em uma tabela interna, chamada de tabela de estados, de modo a permitir que os pacotes de resposta ao serviço correspondente possam voltar para a máquina cliente.

Esta entrada só fica ativa durante um curto intervalo de tempo, ao final do qual ela é removida (este intervalo de tempo é configurado através da janela de configuração de parâmetros, mostrada no capítulo intitulado Configurando os parâmetros do sistema). Desta forma, o administrador não precisa se preocupar com a os pacotes UDP de resposta, sendo necessário apenas configurar as regras para permitir o acesso aos serviços. Isto pode ser feito facilmente, já que todos os serviços possuem portas fixas.

O problema do protocolo FTP:

O FTP é um dos protocolos mais populares da Internet, porém é um dos mais complexos de ser tratado por um firewall. Vamos analisar seu funcionamento:

Para acessar o serviço FTP, inicialmente a máquina cliente abre uma conexão TCP para a máquina servidora na porta 21. (a porta usada pelo cliente é variável). Esta conexão é chamada de conexão de controle. A partir daí, para cada arquivo transferido ou para cada listagem de diretório, uma nova conexão é estabelecida, chamada de conexão de dados. Esta conexão de dados pode ser estabelecida de duas maneiras distintas:

1. O servidor pode iniciar a conexão a partir da porta 20 em direção a uma porta variável, informada pelo cliente pela conexão de controle (este é chamado de **FTP ativo**)
2. O cliente pode abrir a conexão a parir de uma porta variável para uma porta variável do servidor, informada para o cliente através da conexão de controle (este é chamado de **FTP passivo**).

Em ambos os casos o administrador não tem como saber quais portas serão escolhidas para estabelecer as conexões de dados e desta forma, se ele desejar utilizar o protocolo FTP através de um filtro de pacotes tradicional, deverá liberar o acesso para todas as possíveis portas utilizadas pelas máquinas clientes e servidores. Isto tem implicações sérias de segurança.

O Firewall Aker tem a capacidade de vasculhar o tráfego da conexão de controle FTP e desta forma descobrir qual o tipo de transferência será utilizada (ativa ou passiva) e

quais portas serão usadas para estabelecer as conexões de dados. Desta forma, todas as vezes que o filtro de pacotes determina que uma transferência de arquivos será realizada, ele acrescenta uma entrada na tabela de estados de modo a permitir que a conexão de dados seja estabelecida. Esta entrada só fica ativa enquanto a transferência estiver se realizando e caso a conexão de controle esteja aberta, propiciando o máximo de flexibilidade e segurança. Neste caso, para se configurar o acesso FTP, basta se acrescentar uma regra liberando o acesso para a porta da conexão de controle (porta 21). Todo o resto será feito automaticamente.

O problema do protocolo Real Audio:

O protocolo Real Audio é o mais popular protocolo de transferência de som e vídeo em tempo real através da Internet.

Para que seja possível uma transmissão de audio ou vídeo, é necessário que o cliente estabeleça uma conexão TCP para o servidor de Real Audio. Além desta conexão, para conseguir uma melhor qualidade de som, o servidor pode abrir uma conexão UDP para o cliente, para uma porta randômica informada em tempo real pelo cliente e o cliente também pode abrir uma outra conexão UDP para o servidor, também em uma porta randômica informada pelo servidor no decorrer da conexão.

Os filtros de pacotes tradicionais não permitem o estabelecimento das conexões UDP do servidor para o cliente e vice-versa, uma vez que as portas não são conhecidas antecipadamente, fazendo com que a qualidade do audio e vídeo obtidas seja bastante inferior.

O filtro de estados do Firewall Aker, acompanha toda a negociação do servidor Real Audio com o cliente de modo a determinar se as conexões UDP serão abertas, e para quais portas, e acrescenta esta informação em uma entrada na sua tabela de estados. Esta entrada na tabela de estados só fica ativa enquanto a conexão de controle TCP estiver aberta, propiciando um máximo de segurança.

O problema do protocolo Real Video (RTSP):

O protocolo Real Vídeo é suportado pelo firewall. Da mesma maneira que o Real Audio, as transações são controladas pelo firewall, permitindo total segurança do uso de aplicações de Real Vídeo.

Montando regras de filtragem em um filtro de pacotes simples

Antes de mostrar como funciona a configuração do filtro de estados do Firewall Aker, é interessante explicar o funcionamento básico de um filtro de pacotes simples:

Existem vários critérios possíveis para se realizar filtragem de pacotes. A filtragem de endereços pode ser considerada a mais simples de todas: ela consiste em comparar os endereços do pacote com os endereços das regras, caso os endereços sejam iguais o pacote esta aprovado. Esta comparação é feita da seguinte forma:

Trabalharemos com a seguinte regra: Todas as máquinas da rede 10.1.x.x podem se comunicar com as máquinas da rede 10.2.x.x. Escreveremos esta regra utilizando o conceito de mascaramento (para maiores informações, veja o capítulo intitulado Cadastrando Entidades). Assim temos:

```
10.1.0.0 & 255.255.0.0 -> 10.2.0.0 & 255.255.0.0
------- Origem ------     ------- Destino -------
```

Vamos agora aplicar a regra a um pacote que trafega da máquina 10.1.1.2 para a maquina 10.3.7.7. Aplicaremos a máscara da regra aos dois endereços, o da regra e o do pacote e verificamos se os endereços são iguais, tanto o destino quanto o origem.:
Para o endereço origem temos

```
10.1.0.0 AND 255.255.0.0 = 10.1.0.0 (para a regra)
10.1.1.2 AND 255.255.0.0 = 10.1.0.0 (para o pacote)
```

Temos então que os dois endereços origem são iguais após a aplicação da máscara.
Veremos agora para o endereço destino:

```
10.2.0.0 AND 255.255.0.0 = 10.2.0.0 (para a regra)
10.3.7.7 AND 255.255.0.0 = 10.3.0.0 (para o pacote)
```

Como o endereço destino do pacote não está igual ao endereço destino da regra após a aplicação da máscara, por definição, esta regra não se aplicaria a este pacote.
Esta operação é feita em toda a lista de endereços e máscaras destino e origem até o fim da lista, ou até uma das regras se aplicar para o pacote examinado. Uma lista de regras teria a seguinte forma:

```
10.1.1.2 & 255.255.255.255 -> 10.2.0.0 & 255.255.0.0
10.3.3.2 & 255.255.255.255 -> 10.1.2.1 & 255.255.255.255
10.1.1.0 & 255.0.0.0       -> 10.2.3.0 & 255.255.255.0
10.1.0.0 & 255.255.0.0     -> 10.2.0.0 & 255.255.0.0
```

Além dos endereços origem e destino, cada pacote IP possui um protocolo e um serviço associados. Esta combinação serviço mais protocolo pode ser utilizado como mais um critério de filtragem.

Os serviços no protocolo TCP, por exemplo, estão sempre associados a uma porta (para maiores informações, veja o capítulo intitulado Cadastrando Entidades). Assim, pode-se também associar uma lista de portas aos endereços.

Pegaremos como exemplo dois serviços conhecidos, o POP3 e o HTTP. O POP3 está associado à porta 110 do servidor e o HTTP está associado à porta 80. Assim, iremos acrescentar estas portas no formato da regra. Teremos então:

```
10.1.0.0 & 255.255.0.0 -> 10.2.0.0 & 255.255.0.0       TCP       80
110
------- Origem ------     ------- Destino ------- - Protocolo - --
Portas--
```

Esta regra autoriza todo pacote que vai da rede 10.1.x.x para a rede 10.2.x.x e que utiliza os serviços HTTP ou POP3 a trafegar pelo firewall.

Assim, em uma primeira etapa compara-se os endereços da regra com os do pacote. Caso estes endereços sejam iguais após a aplicação das máscaras, passa-se a comparar o protocolo e a porta destino no pacote com o protocolo e a lista de portas associados à regra. Se o protocolo for o mesmo e se for encontrada uma porta da regra igual à porta do pacote, esta regra por definição se aplica ao pacote, caso contrário a pesquisa continua na próxima regra.

Assim um conjunto de regras teria o seguinte formato

```
10.1.1.2 & 255.255.255.255 -> 10.2.0.0 & 255.255.0.0     UDP 53
10.3.3.2 & 255.255.255.255 -> 10.1.2.1 & 255.255.255.255 TCP 80
10.1.1.0 & 255.0.0.0       -> 10.2.3.0 & 255.255.255.0   TCP 21 20 113
10.1.0.0 & 255.255.0.0     -> 10.2.0.0 & 255.255.0.0     ICMP 0 8
```

Montando regras de filtragem para o Firewall Aker

Configurar as regras de filtragem no Firewall Aker é algo muito fácil em função de sua concepção inteligente. Toda a parte de endereços IP, máscaras, protocolos, portas e interfaces é configurada nas entidades (para maiores informações, veja o capítulo intitulado Cadastrando Entidades). Devido a isso, ao configurar uma regra, não é necessário se preocupar com qual porta um determinado serviço utiliza ou qual o endereço IP de uma rede. Tudo isso já foi previamente cadastrado. Para facilitar ainda mais, todos os serviços mais utilizados na Internet já vem previamente configurados de fábrica, sendo desnecessário perder tempo pesquisando os dados de cada um.

Basicamente, para cadastrar uma regra, o administrador deve especificar as entidades de origem, destino e os serviços que farão parte da regra. Ele pode também especificar uma interface de origem para os pacotes e definir em quais horários a regra estará ativa, em uma tabela de horários semanal. Com o uso desta tabela de horários é possível liberar determinados serviços em determinadas horas do dia (por exemplo, liberar IRC, ou bate-papo, apenas nos horários fora do expediente). Se um pacote chegar em um horário no qual a regra não está marcada como ativa ela será ignorada, fazendo com que a busca continue na próxima regra da lista.

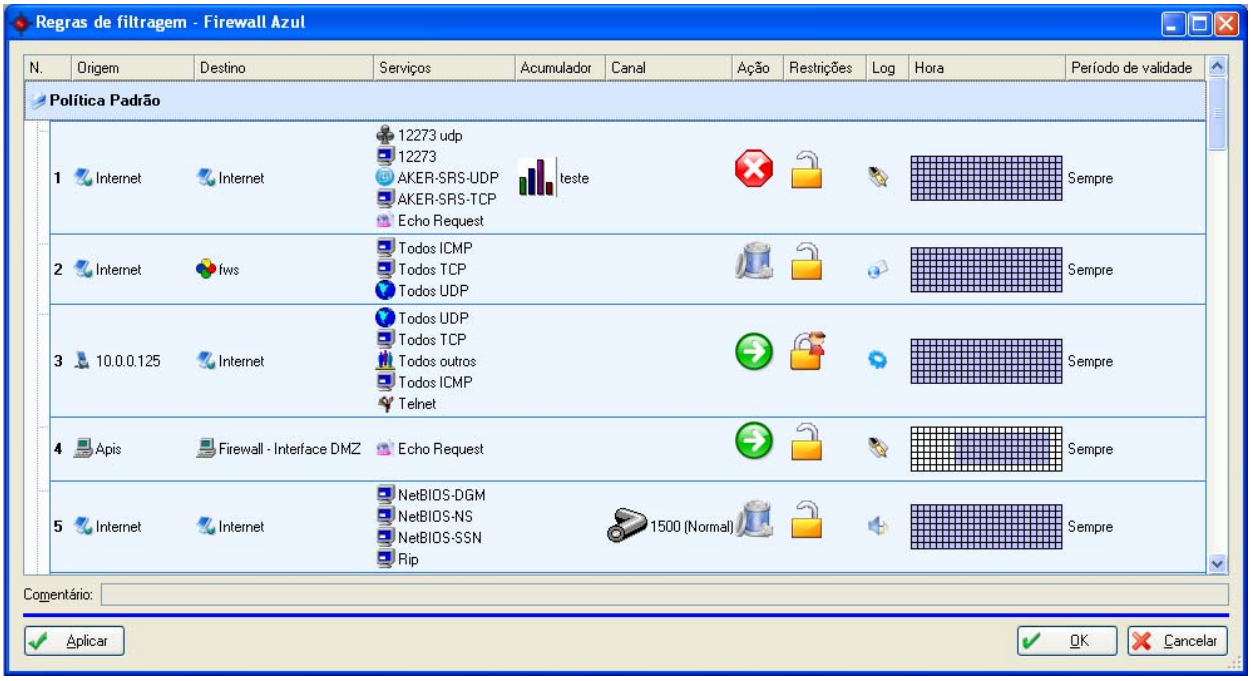
O funcionamento do filtro é simples: o firewall irá pesquisar uma a uma as regras definidas pelo administrador, na ordem especificada, até que o pacote se encaixe numa delas. A partir deste momento, ele irá executar a ação associada à regra, que pode ser aceita, rejeita ou descarta (estes valores serão explicados no próximo tópico). Caso a pesquisa chegue ao final da lista e o pacote não se enquadre em nenhuma regra então este será descartado (é possível se configurar ações para serem executadas neste caso. Isto será tratado no capítulo intitulado Configurando as ações do sistema).

6-2 Editando uma lista de regras usando a interface gráfica

Para ter acesso a janela de configuração de regras basta:

- Clicar no menu *Configurações do firewall* da janela principal
- Selecionar o item *Regras de Filtragem*

A janela de regras de filtragem

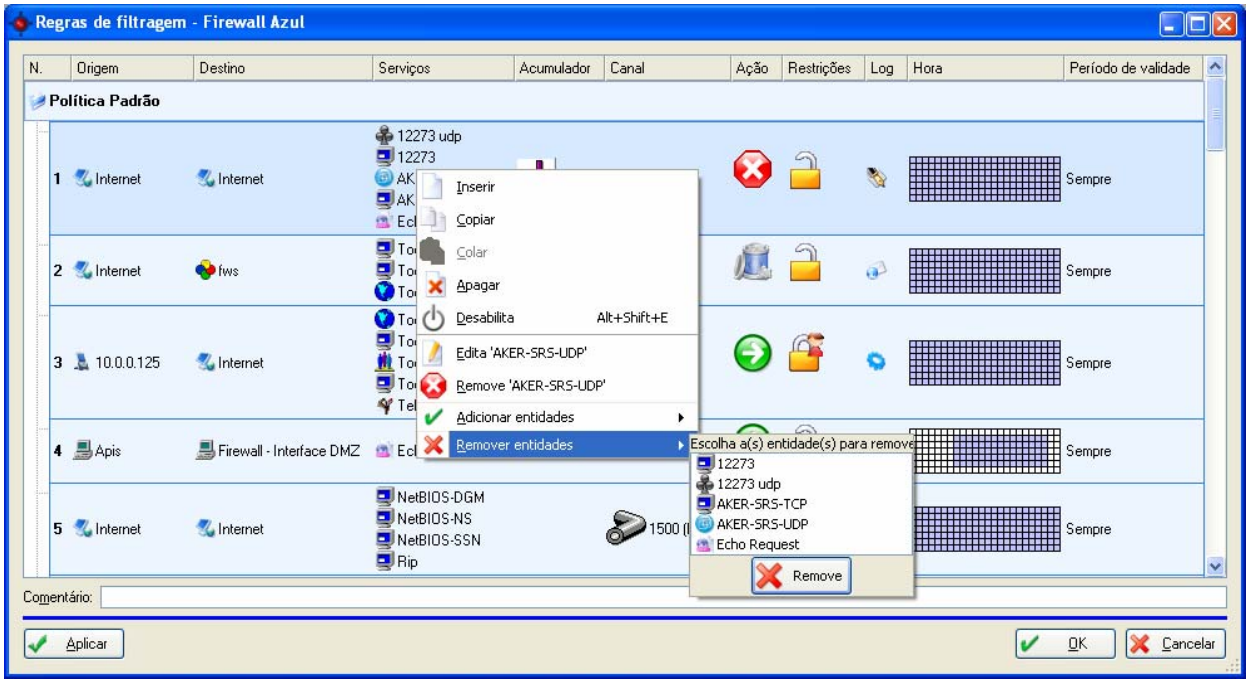


A janela de regras contém todas as regras de filtragem definidas no Firewall Aker. Cada regra será mostrada em uma linha separada, composta de diversas células. Caso uma regras esteja selecionada, ela será mostrada em uma cor diferente.

- O botão **OK** fará com que o conjunto de regras seja atualizado e passe a funcionar imediatamente.
- O Botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

- Ao se clicar sobre uma regra e selecioná-la, se ela possuir um comentário, este aparecerá na parte inferior da janela.

Para se executar qualquer operação sobre uma determinada regra, basta clicar com o botão direito do mouse sobre o campo que se deseja alterar . Aparecerá um menu com as opções de entidades referentes ao campo, como na figura abaixo:



- **Inserir:** Esta opção permite se incluir uma nova regra na lista. Se alguma regra estiver selecionada, a nova será inserida na posição da regra selecionada. Caso contrário, a nova regra será incluída no final da lista.
- **Apagar**: Esta opção remove da lista a regra selecionada.
- **Copiar:** Esta opção copia a regra selecionada para uma área temporária.
- **Colar:** Esta opção copia a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.
- **Habilitada:** Esta opção permite desabilitar/habilitar a regra selecionada.
- **Adicionar entidades:** Adiciona uma entidade cadastrada no firewall. Veja se o ponteiro do mouse está sobre o campo o qual se quer inserir a entidade.
- **Remover entidades**: Remove uma entidade que foi inserida na regra.

Dica: A posição de cada regra pode ser alterada, bastando clicar e arrastar a mesma para a nova posição desejada, soltando em seguida.

Adicionando e removendo entidades e serviços na regra

Para se adicionar uma entidade a um destes campos, pode-se proceder de duas formas:

1. Seleciona-se a entidade a ser incluída, clicando-se sobre ela na tabela de entidades, localizada na parte inferior esquerda da janela, e arraste-a para o campo correspondente. As teclas *Insert* e *Delete* podem inserir e remover as entidades respectivamente.
2. Clica-se com o botão direito do mouse sobre o campo onde se deseja adicionar as entidades, será exibida uma lista das entidades pertinentes ao campo selecionado, bem como que tipo de ação se deseja aplicar sobre as mesmas.
3. O duplo-clique na entidade irá permitir a edição da mesma.

Para se remover uma entidade de um destes campos, deve-se proceder da seguinte forma:

1. Clica-se com o botão direito do mouse sobre o campo onde se encontra a entidade que se deseja remover e será exibida uma lista das entidades participantes do campo com a opção de remoção da entidades no seguinte formato: **remover 'entidade_removida'.**
2. Pode-se utilizar a opção **Remover Entidade** para eliminar várias entidades de uma vez.

- **Parâmetros da regra:**

Além das especificações básicas de uma regra como: entidades de origem, entidades de destino e serviços devemos levar em conta outros parâmetros de configuração:

Acumulador: Define qual o acumulador para os pacotes da regra. A opção *nenhum* desativa a contabilização dos pacotes que se encaixem nesta regra. Se for escolhido um acumulador, serão adicionados a ele a quantidade de bytes e pacotes encaixados nesta regra.

Canal: Define o canal que será utilizado para controlar a banda para a regra. A opção *nenhum* desativa a utilização de controle de banda para esta regra

Ação: Este campo define qual a ação a ser tomada para todos os pacotes que se encaixem nesta regra. Ela consiste nas seguintes opções:
Aceita: Significa que os pacotes que se encaixarem neste regra serão autorizados a passar através do firewall.

Rejeita: Significa que os pacotes que se encaixarem nesta regra não passarão pelo firewall e será enviado um pacote ICMP para a máquina de origem do pacote dizendo que o destino é inatingível. Esta opção não funciona para alguns tipos de serviço ICMP, devido a uma característica inerente a este protocolo.

Descarta: Significa que os pacotes que se encaixarem nesta regra não passarão pelo firewall, mas não será enviado nenhum pacote para a máquina de origem.

Restrições: Este campo permite que se especifique exigências adicionais que um pacote deve cumprir para que ele se encaixe nesta regra. Ele é formado pelas seguintes opções:
Nenhum: Não existe nenhuma exigência adicional.

Somente se encriptado: Neste caso, para que um pacote se enquadre nesta regra, ele deverá obrigatoriamente vir encriptado/autenticado, ou seja, vir de um canal seguro. Esta opção é particularmente útil quando se está utilizando clientes de criptografia e se deseja que apenas conexões provenientes destes clientes (ou de canais de criptografia firewall-firewall) sejam aceitas. Para maiores informações sobre criptografia e canais seguros, veja o capítulo Criando canais de criptografia.

Somente se encriptado e de um usuário autenticado: Neste caso, para que os pacotes sejam aceitos, além deles virem encriptados/autenticados, o usuário que estabeleceu o canal seguro deve ter sido autenticado pelo firewall. A única maneira de um pacote atender esta exigência é ele ser proveniente de um cliente de criptografia e a opção de realizar autenticação de usuários para os clientes de criptografia estar ativa. Para

maiores informações sobre criptografia e canais seguros, veja o capítulo Criando canais de criptografia.

Log: Este campo define que tipos de ações serão executadas pelo sistema quando um pacote se encaixar nesta regra. Ele consiste de várias opções que podem ser selecionadas independentemente uma das outras. Os valores possíveis são:
Logs: Se esta opção estiver selecionada, todos os pacotes que se enquadrarem nesta regra serão registrados no log do sistema.

Envia email: Se esta opção estiver selecionada, será enviado um e-mail todas as vezes que um pacote se enquadrar nesta regra (a configuração do endereço de e-mail será mostrada no capítulo intitulado configurando as ações do sistema).

Executar programa: Se esta opção estiver marcada, será executado um programa definido pelo administrador todas as vezes que um pacote se enquadrar nesta regra (a configuração do nome do programa a ser executado será mostrada no capítulo intitulado configurando as ações do sistema).

Disparar mensagens de alarme: Se esta opção estiver selecionada, o firewall mostrará uma janela de alerta todas as vezes que um pacote se enquadrar nesta regra. Esta janela de alerta será mostrada na máquina onde a interface gráfica remota estiver aberta e, se a máquina permitir, será emitido também um aviso sonoro. Caso a interface gráfica não esteja aberta, não será mostrada nenhuma mensagem e esta opção será ignorada.

Enviar Trap SMNP: Se esta opção estiver selecionada, será enviada uma Trap SNMP para cada pacote que se enquadrar nesta regra (a configuração dos parâmetros para o envio das traps será mostrada no capítulo intitulado configurando as ações do sistema).

No caso do protocolo TCP, somente serão executadas as ações definidas na regra para o pacote de abertura de conexão. No caso do protocolo UDP, todos os pacotes que forem enviados pela máquina cliente e se enquadrarem na regra (porém não os pacotes de resposta) provocarão a execução das ações.
Tabela de horários: Esta tabela define as horas e dias da semana em que a regra é aplicável. As linhas representam os dias da semana e as colunas as horas. Caso se queira que a regra seja aplicável em determinada hora o quadrado deve ser preenchido, caso contrário o quadrado deve ser deixado em branco.

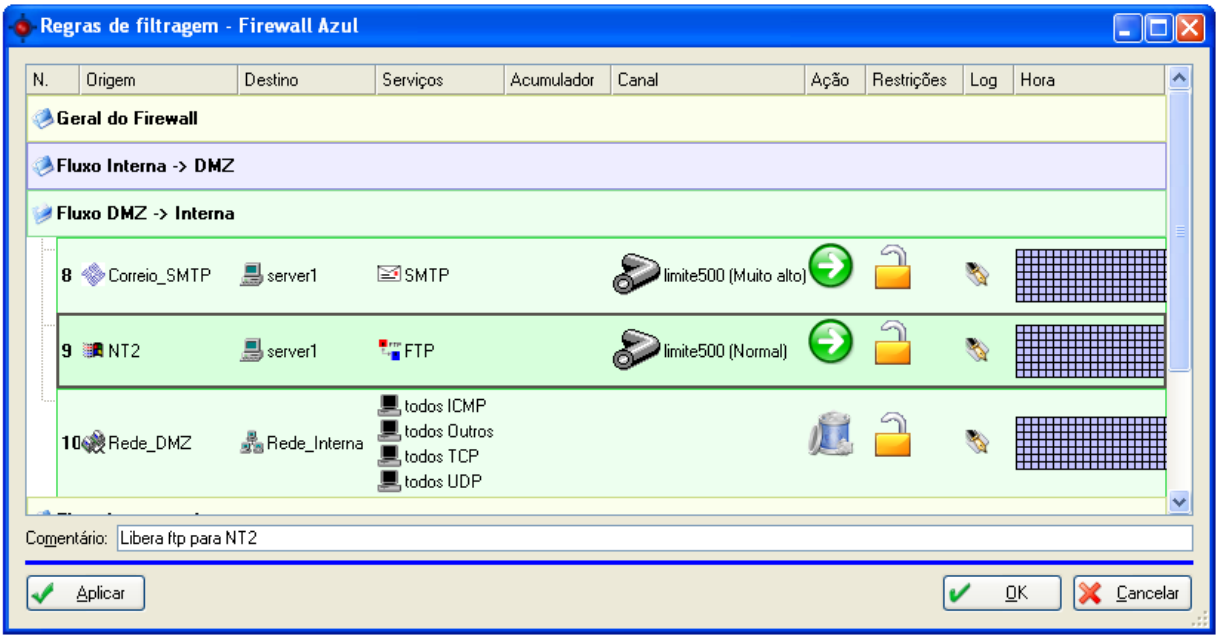
Para facilitar sua configuração, pode-se clicar com o botão esquerdo do mouse sobre um quadrado e a seguir arrastá-lo, mantendo o botão pressionado. Isto faz com que o a tabela seja alterada na medida em que o mouse se move.

Período de validade: Permite o cadastro de duas datas que delimitam um período fora do qual a regra não tem validade. É um recurso muito útil para, por exemplo, liberar o tráfego relacionado a um evento não recorrente, como um teste. Se o período ainda não tiver começado ou estiver expirado, o número da regra será mostrado sobre um fundo vermelho.

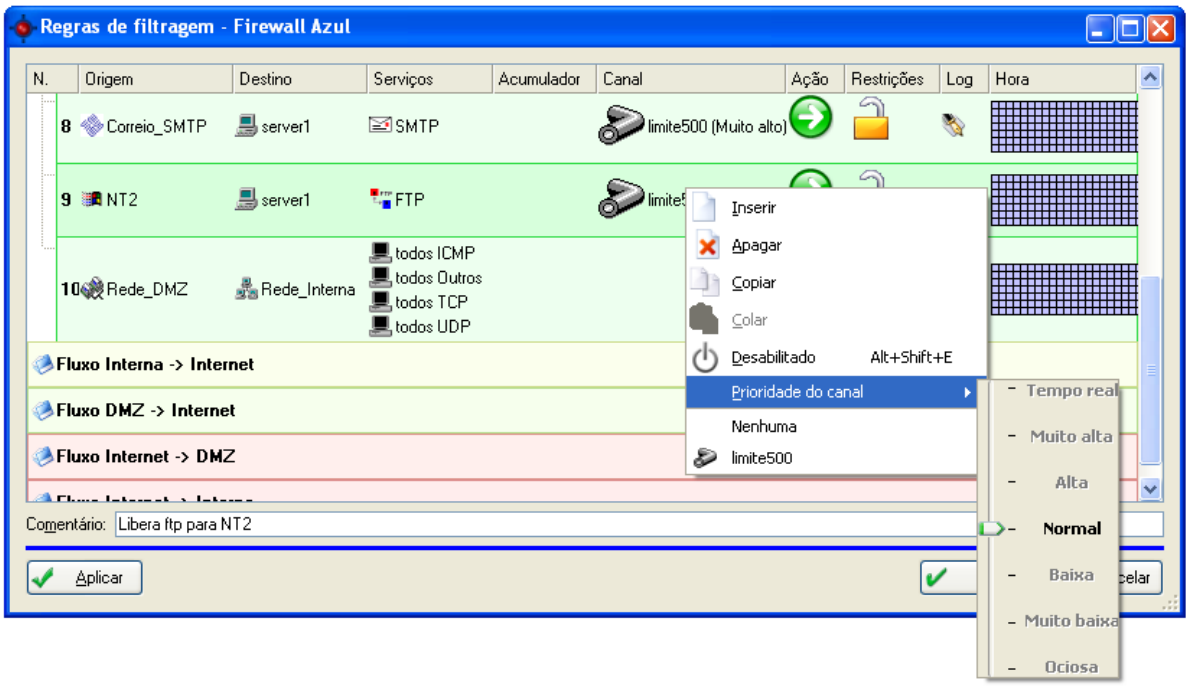
<>**Comentário:** Reservado para se colocar um comentário sobre a regra. Muito útil na documentação e manutenção das informações sobre a utilidade da regra.

Utilização dos Canais na Regra de Filtragem do Firewall Aker

O administrador pode definir Qualidade de Serviço (QoS) diferenciada para cada tipo de regra. No caso da figura abaixo, foi criado um canal de 500Kbits e aplicado nas regras 8 e 9. O servidor "Correio_SMTP" possui prioridade no tráfego pois a prioridade para ele no canal está como "Muito alto".



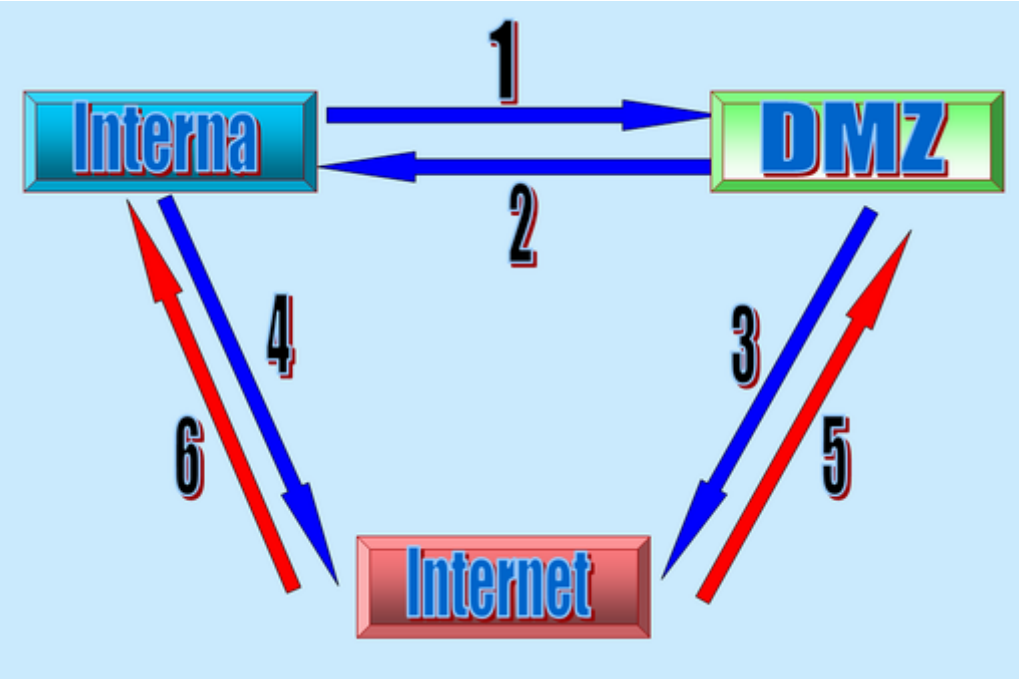
Para ajustes de prioridade de canal, basta clicar como o botão direito na entidade Canal e escolher a prioridade pelo botão deslizando. Veja a figura abaixo:



6-3 Trabalhando com Políticas de Filtragem

Uma nova implementação foi inserida na configuração das regras de filtragem do firewall, que é o uso de Políticas de Filtragem. Este recurso permite que o administrador do firewall faça um agrupamento de regras dentro de um levantamento feito dos fluxos que ocorrerem entre as suas sub redes.

Para exemplificar, suponha que o administrador possua um firewall colocado entre as redes interna, DMZ e Internet, conforme esquema abaixo:



Pode-se verificar os possíveis fluxos de dados que poderão ocorrer entre essas redes. Para cada fluxo foi dada uma numeração e com isso pode-se concluir que os fluxos com números mais altos (5 e 6) serão considerados os mais inseguros, pois envolvem o acesso da internet as redes DMZ e interna, respectivamente.

Estes fluxos para o firewall serão desdobrados em regras de filtragem, com isto poderia se ter as seguintes regras:

Regras de Filtragem

N.	Origem	Destino	Serviços	Acumulador	Canal	Ação	Restrições	Lo
1	Maquina_Admin	Firewall_Interno	Aker					
2	Internet	Internet	Echo Reply Echo Request					
3	Internet	Firewall Externo	Aker-CDP Aker-CL					
4	Internet	Firewall Externo Firewall_Interno Firewall DMZ	todos TCP todos UDP todos ICMP todos Outros					
5	server1	Correio_SMTP	SMTP					
6	Rede_Interna	servidor_web	HTTP					
7	Rede_Interna	Rede_DMZ	todos ICMP todos Outros todos TCP					

			todos UDP				
8	Correio_SMTP	server1	SMTP				
9	NT2	server1	FTP				
10	Rede_DMZ	Rede_Interna	todos ICMP todos Outros todos TCP todos UDP				
11	Rede_Interna	Server_pop3	POP3				
12	squid_proxy	Internet	HTTP HTTPS				
13	Rede_Interna	Internet	todos ICMP todos Outros todos TCP todos UDP				
14	NT1	Internet	DNS DNS (TCP)				
15	NT3	Rede_Verde	FTP				

16	Rede_DMZ	Internet	todos ICMP todos Outros todos TCP todos UDP				
17	Internet	NT3	DNS (TCP) DNS				
18	Internet	servidor_web	HTTP				
19	Internet	Rede_DMZ	todos ICMP todos Outros todos TCP todos UDP				
20	Internet	Rede Interna	todos ICMP todos Outros todos TCP todos UDP				

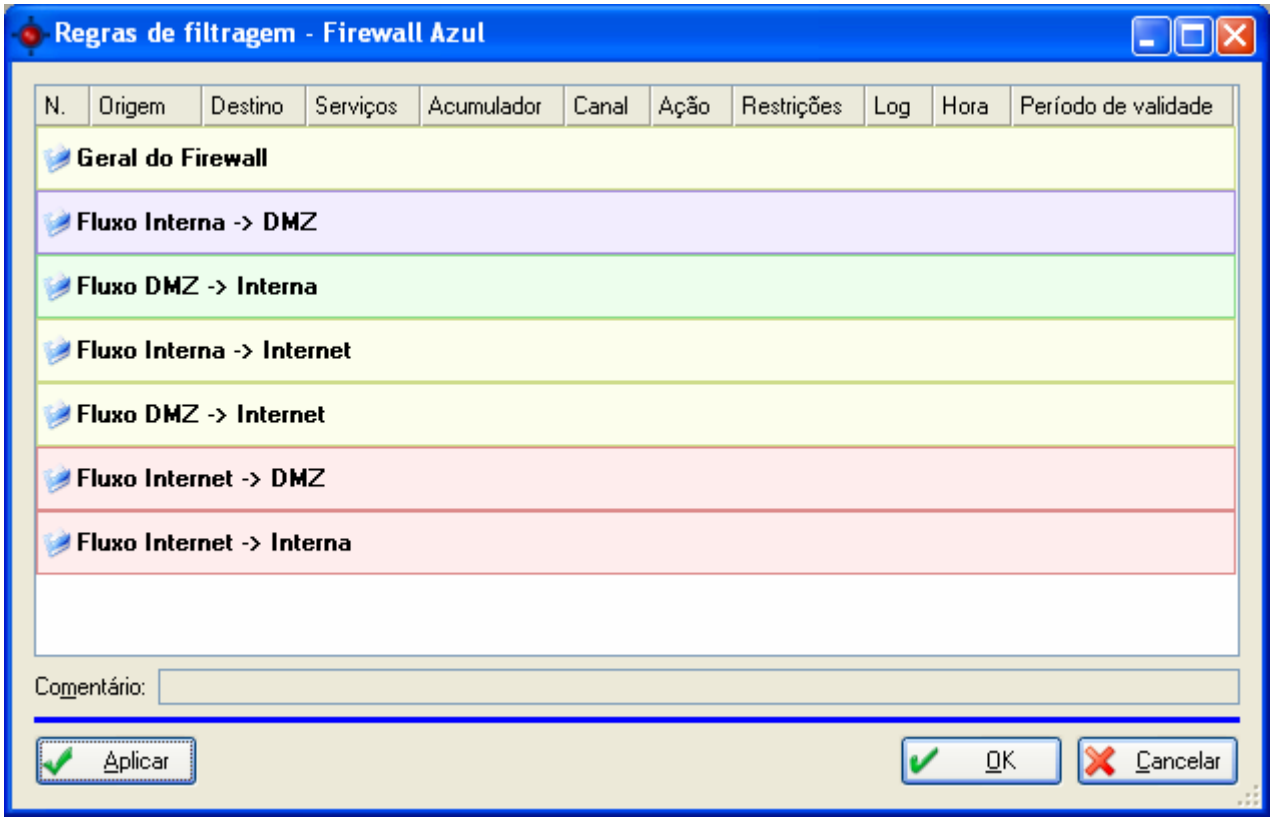
No exemplo acima foi criado as seguintes regras:

Regras Gerais do Firewall -> 1 a 4
Fluxo Interna para DMZ -> 5 a 7
Fluxo DMZ para Interna -> 8 a 10
Fluxo Interna para Internet -> 11 a 13
Fluxo DMZ para Internet -> 14 a 16
Fluxo Internet para DMZ -> 17 a 19
Fluxo Internet para Interna -> 20

Repare que ao final de cada fluxo foi colocado uma regra bloqueando o mesmo (4, 7, 10, 13, 16, 19 e 20). O objetivo desta técnica é para evitar que erros cometidos ao longo do cadastramento das regras de filtragem possam abrir inadiverditamente um acesso não permitido, com isso caso uma regra não esteja colocada corretamente dentro do fluxo fatalmente ela cairá em um destes bloqueios que não permitirá o acesso indevido.

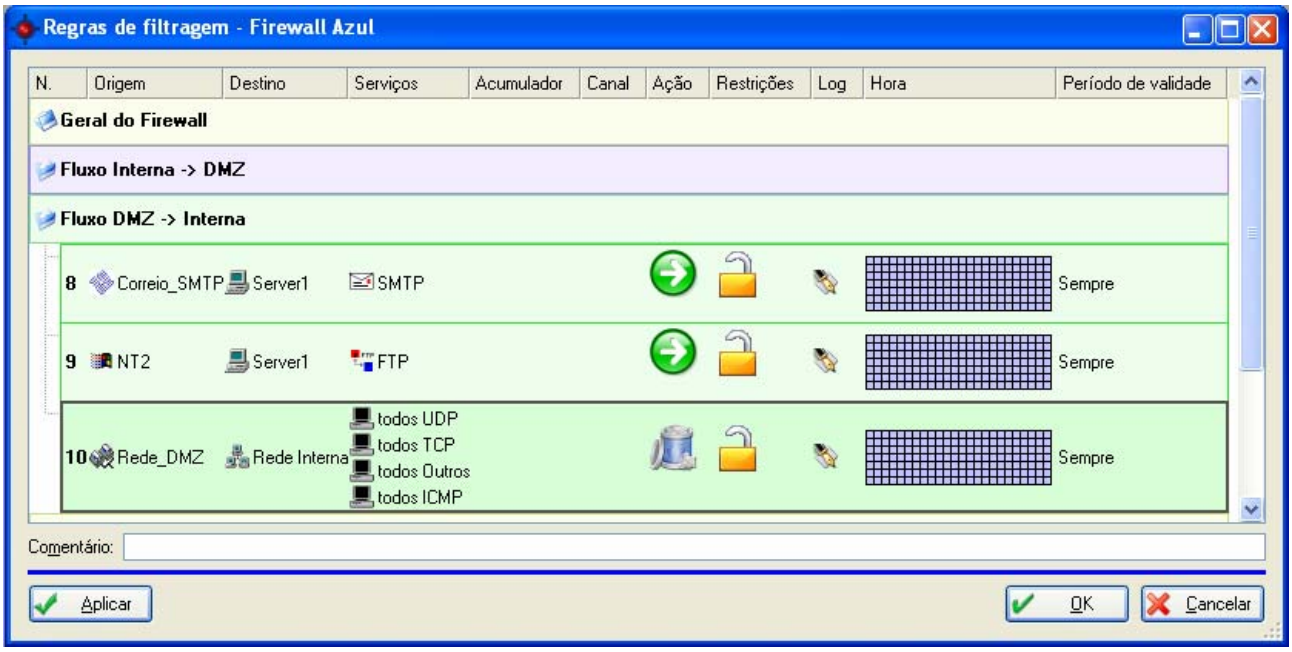
Observe que no fluxo Internet para Rede Interna não existe nenhuma regra cadastrada, apenas o bloqueio.

Para melhor visualização e controle, o firewall permite agrupar estas regras pelos fluxos. A interface então ficaria desta forma:



Para criar as Políticas basta clicar no ícone da barra de ferramentas "Política".

A figura abaixo mostra o desdobramento das regras da política. Basta dar um duplo clique na linha para exibir as regras que ela contém:



No caso de desabilitar uma política, todas as regras que ela contém também serão desabilitadas.

6-4 Utilizando a interface texto

A utilização da interface texto na configuração das regras de filtragem traz uma dificuldade gerada pela grande quantidade de parâmetros que devem ser passados pela linha de comando.

Não é possível se configurar a tabela de horários nem se especificar comentários para as regras através da interface texto. Também não é possível se especificar mais de uma entidade para origem ou destino da regra. Todas as regras acrescentadas por esta interface são consideradas aplicáveis em todas as horas da semana.

Localização do programa: `/etc/firewall/fwrule`

Sintaxe:

```
Uso: fwrule [ajuda | mostra]
     fwrule [habilita | desabilita | remove] <pos>
     fwrule inclui [forca] <pos> <origem> <destino>\
                   <aceita | rejeita | descarta>\
                   [pipe <pipe> <peso>] [acumulador <acumulador>]
                   [loga] [mail] [trap] [programa] [alerta]
                   [encriptado | usuario ] [<servico> ...]
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
fwrule - Configura tabela de regras do filtro de estados
Uso: fwrule [ajuda | mostra]
     fwrule [habilita | desabilita | remove] <pos>
     fwrule inclui [forca] <pos> <origem> <destino>\
```

```
                    <aceita | rejeita | descarta>\
                    [pipe <pipe> <peso>] [acumulador <acumulador>]
                    [loga] [mail] [trap] [programa] [alerta]
                    [encriptado | usuario ] [<servico> ...]

     mostra     = mostra todas as entradas da tabela de regras
     inclui     = inclui uma nova regra de filtragem
     habilita   = habilita uma regra de filtragem desabilitada
     desabilita = desabilita uma regra de filtragem existente
     remove     = remove uma regra existente
     ajuda      = mostra esta mensagem

Para inclui temos:
     pos        = posicao onde incluir a nova regra na tabela
                  (Pode ser um inteiro positivo ou a palavra FIM para
incluir
                   no final da tabela)
     aceita     = a regra aceita as conexoes que se enquadrarem nela
     rejeita    = a regra rejeita as conexoes que se enquadrarem nela
e envia
                  pacote ICMP de destino inatingivel para maquina de
origem
     descarta   = a regra descarta os pacotes recebidos (nao envia
pacote ICMP)
     pipe       = faz com que o trafego que se encaixe nesta regra
seja
                  direcionado ao "pipe" indicado com peso relativo
dado por:
     acumulador = faz com que o trafego que se encaixe nesta regra
seja
                  somado a entidade acumulador especificada
     peso       = "ocioso", "m_baixo" (muito baixo), "baixo",
"normal",
                  "alto", "m_alto" (muito alto) ou "tr" (tempo real)
     loga       = loga os pacotes que se enquadrarem na regra
     mail       = envia e-mail para cada pacote que se enquadre na
regra
     trap       = gera trap SNMP para cada pacote que se enquadre na
regra
     programa   = executa um programa para cada pacote que se enquadre
na regra
     alerta     = abre uma janela de alerta para cada pacote que se
enquadre
                  na regra
     encriptado = indica que a regra so e' valida se os pacotes vierem
                  encriptados
     usuario    = indica que a regra so e' valida se os pacotes vierem
                  encriptados e o usuario tiver se autenticado
previamente no
                  firewall. Esta condicao somente pode ser atendida
por
                  conexoes originadas de clientes de criptografia
     servico    = lista de nomes dos servicos para a nova regra

Para habilita / desabilita / remove temos:
     pos        = numero da regra a ser habilitada, desabilitada ou
removida
```

Exemplo 1: (visualizando as regras de filtragem)

```
#/etc/firewall/fwrule mostra

Regra 01
```

```
--------
Origem     : Internet
Destino    : firewall                          cache
Acao       : Descarta
Log        : Loga Trap Alerta
Servicos   : todos_tcp                         todos_udp
             todos_icmp

Regra 02
--------
Origem     : cache                             firewall
Destino    : Internet
Acao       : Aceita
Log        : Loga
Servicos   : http                              ftp

Regra 03
--------
Origem     : Internet
Destino    : Mail server
Acao       : Aceita
Log        : Loga
Servicos   : smtp

Regra 04
--------
Origem     : Empresas externas
Destino    : Aker
Acao       : Aceita
Log        : Loga
Servicos   : smtp
```

Exemplo 2: (removendo a quarta regra de filtragem)

```
#/etc/firewall/fwrule remove 4
Regra 4 removida
```

Exemplo 3: (incluindo uma nova regra no final da tabela)

```
#/etc/firewall/fwrule inclui fim Internet "Mail server" aceita loga
smtp
Regra incluida na posicao 4
```

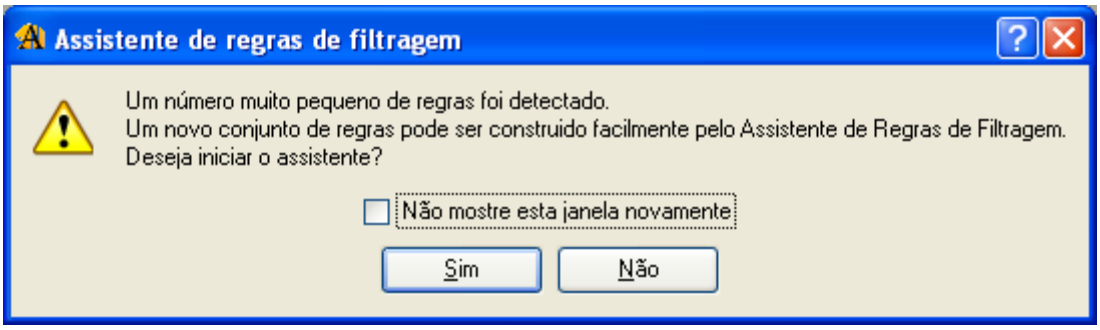
As entidades *Internet* e *Mail server*, bem como o serviço *smtp devem* ter sido previamente cadastradas no sistema. Para maiores informações sobre como cadastrar entidades no Firewall Aker, veja o capítulo entitulado Cadastrando Entidades.

O uso de "" ao redor do nome da entidade a ser incluída na regra é obrigatório quando este contém espaços.

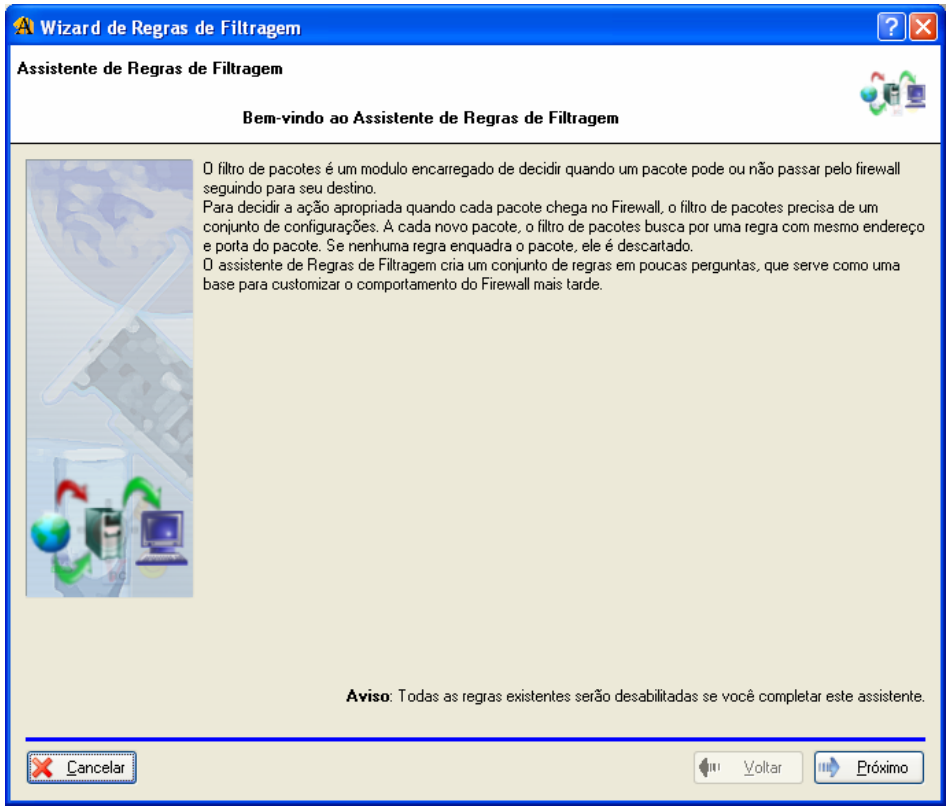
6-5 Utilizando o assistente de regras

O assistente de regras pode ser acionado pelo menu ou pela barra de tarefas. Caso o número de regras for muito pequeno o próprio assistente será acionado automaticamente.

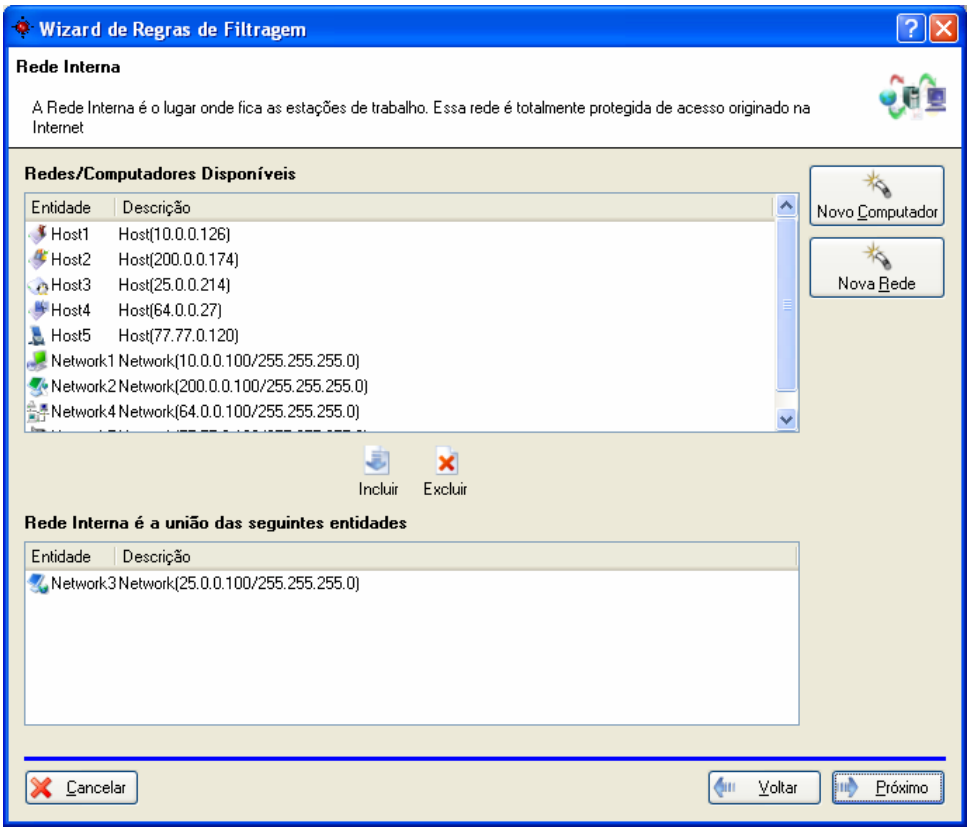
1 - Acionando do assistente de regras. A janela abaixo aparecerá quando um número muito pequeno de regras for detectado.


Assistente de regras de filtragem
Um número muito pequeno de regras foi detectado.
Um novo conjunto de regras pode ser construido facilmente pelo Assistente de Regras de Filtragem.
Deseja iniciar o assistente?
Não mostre esta janela novamente
Sim
Não

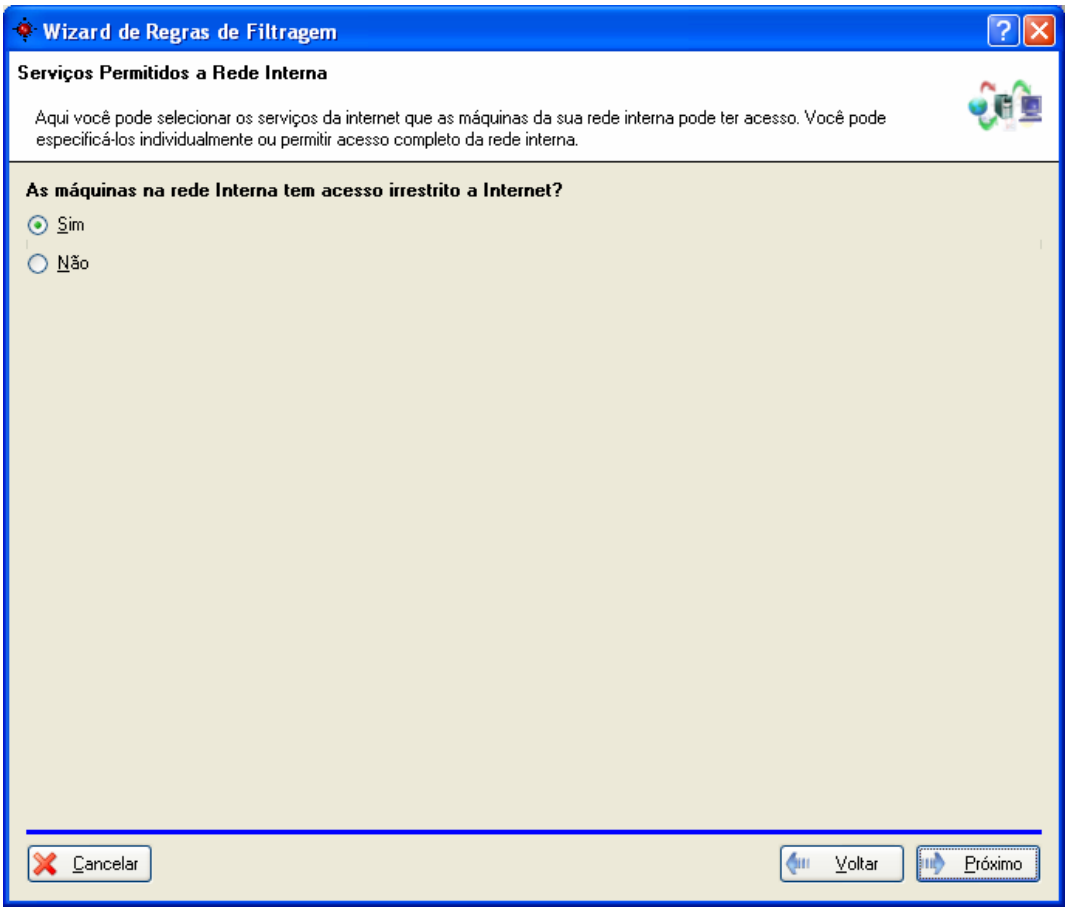
2 - Tela inicial com as explicações necessárias.


Wizard de Regras de Filtragem
Assistente de Regras de Filtragem
Bem-vindo ao Assistente de Regras de Filtragem
O filtro de pacotes é um modulo encarregado de decidir quando um pacote pode ou não passar pelo firewall seguindo para seu destino.
Para decidir a ação apropriada quando cada pacote chega no Firewall, o filtro de pacotes precisa de um conjunto de configurações. A cada novo pacote, o filtro de pacotes busca por uma regra com mesmo endereço e porta do pacote. Se nenhuma regra enquadra o pacote, ele é descartado.
O assistente de Regras de Filtragem cria um conjunto de regras em poucas perguntas, que serve como uma base para customizar o comportamento do Firewall mais tarde.
Aviso: Todas as regras existentes serão desabilitadas se você completar este assistente.
Cancelar
Voltar
Próximo

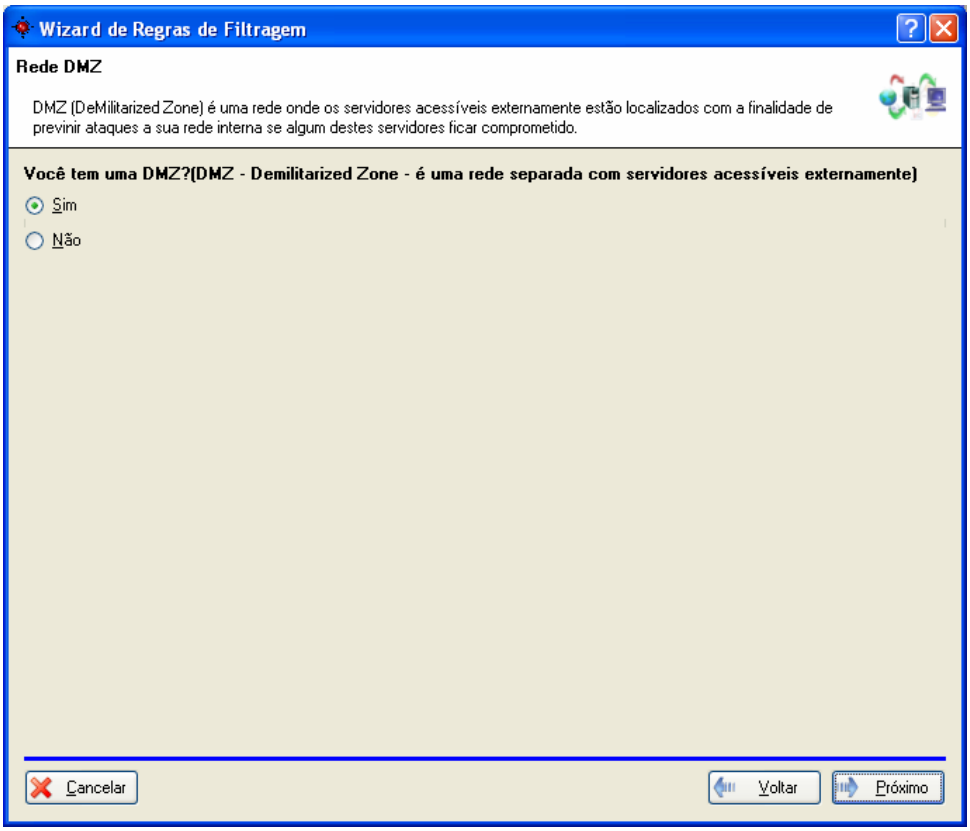
3 - Escolha da rede interna na configuração incial



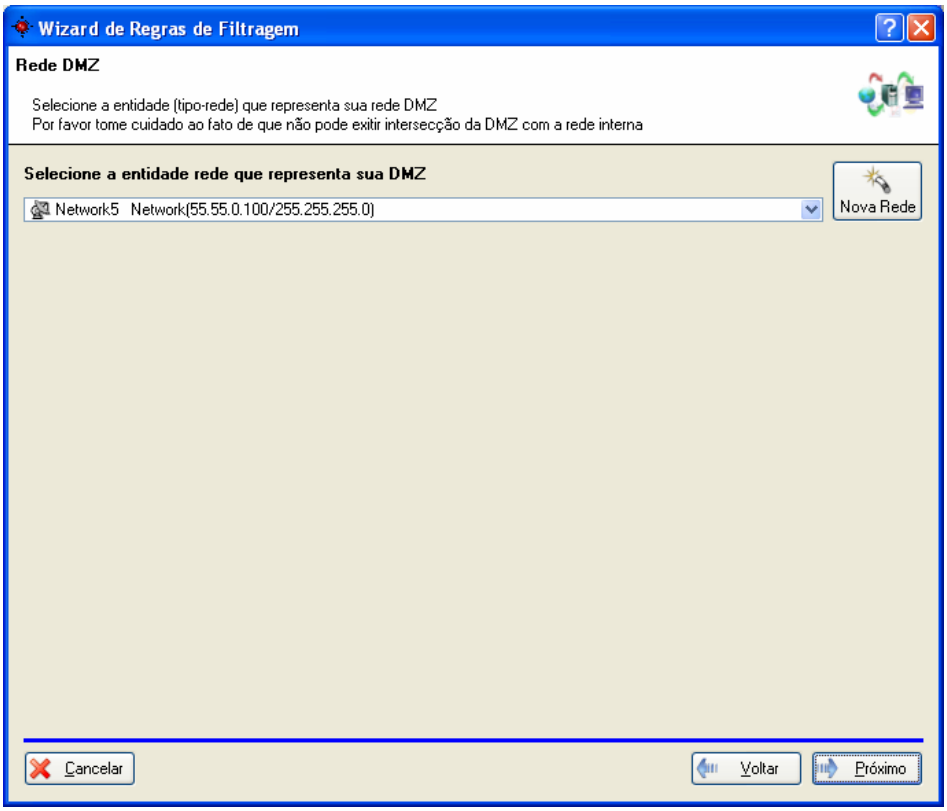
4 - Informação necessária para saber se as máquinas terão acesso irrestrito a Internet.


Wizard de Regras de Filtragem
Serviços Permitidos a Rede Interna
Aqui você pode selecionar os serviços da internet que as máquinas da sua rede interna pode ter acesso. Você pode especificá-los individualmente ou permitir acesso completo da rede interna.
As máquinas na rede Interna tem acesso irrestrito a Internet?
Sim
Não
Cancelar
Voltar
Próximo

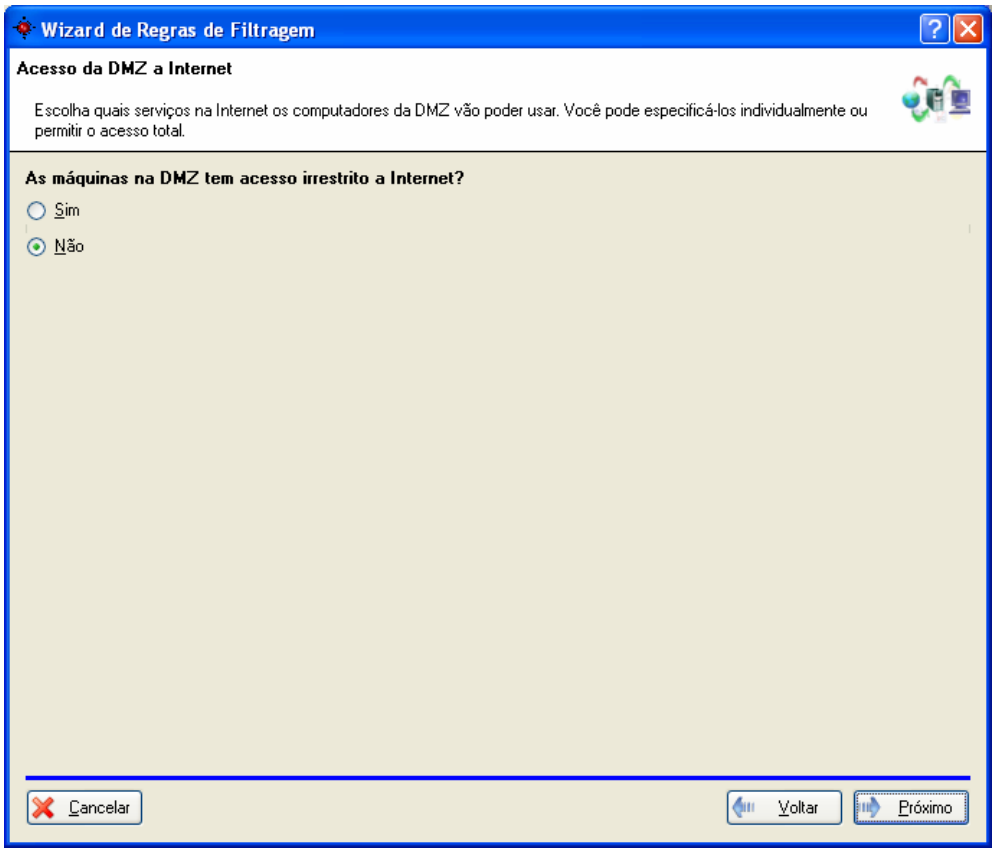
5 - Configuração da DMZ


Wizard de Regras de Filtragem
Rede DMZ
DMZ (DeMilitarized Zone) é uma rede onde os servidores acessíveis externamente estão localizados com a finalidade de previnir ataques a sua rede interna se algum destes servidores ficar comprometido.
Você tem uma DMZ?(DMZ - Demilitarized Zone - é uma rede separada com servidores acessíveis externamente)
Sim
Não
Cancelar
Voltar
Próximo

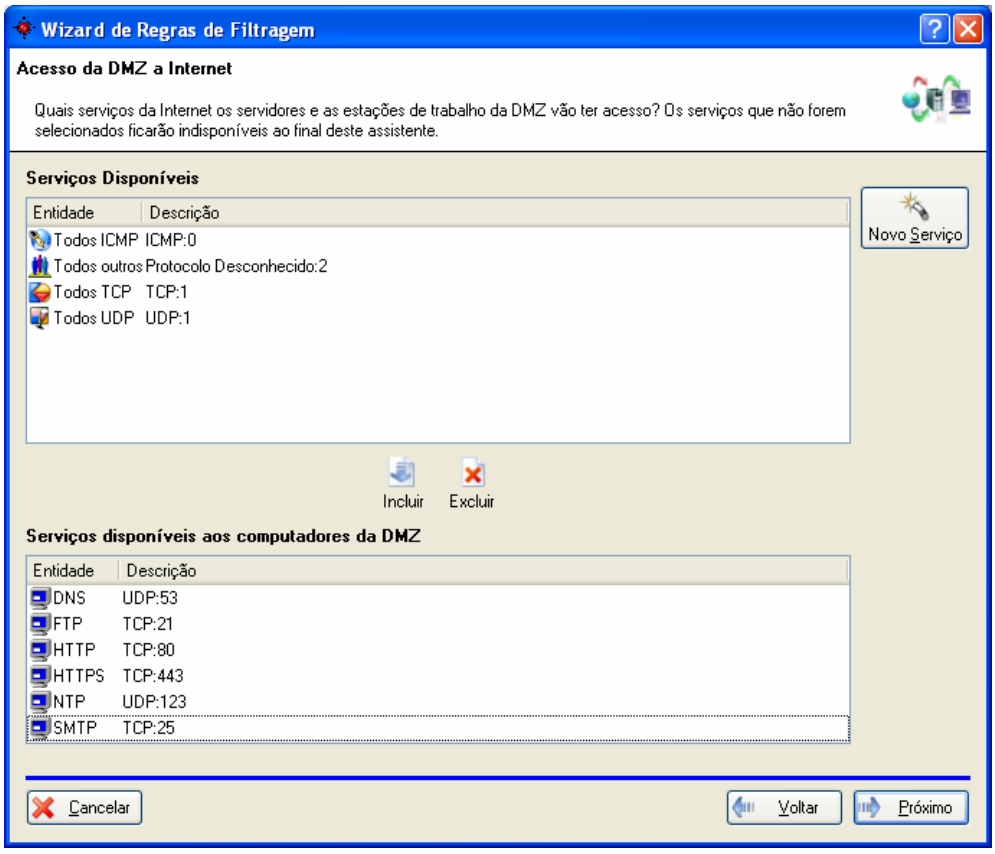
6 - Escolha da entidade da DMZ


Wizard de Regras de Filtragem
Rede DMZ
Selecione a entidade (tipo-rede) que representa sua rede DMZ
Por favor tome cuidado ao fato de que não pode exitir intersecção da DMZ com a rede interna
Selecione a entidade rede que representa sua DMZ
Network5 Network(55.55.0.100/255.255.255.0)
Nova Rede
Cancelar
Voltar
Próximo

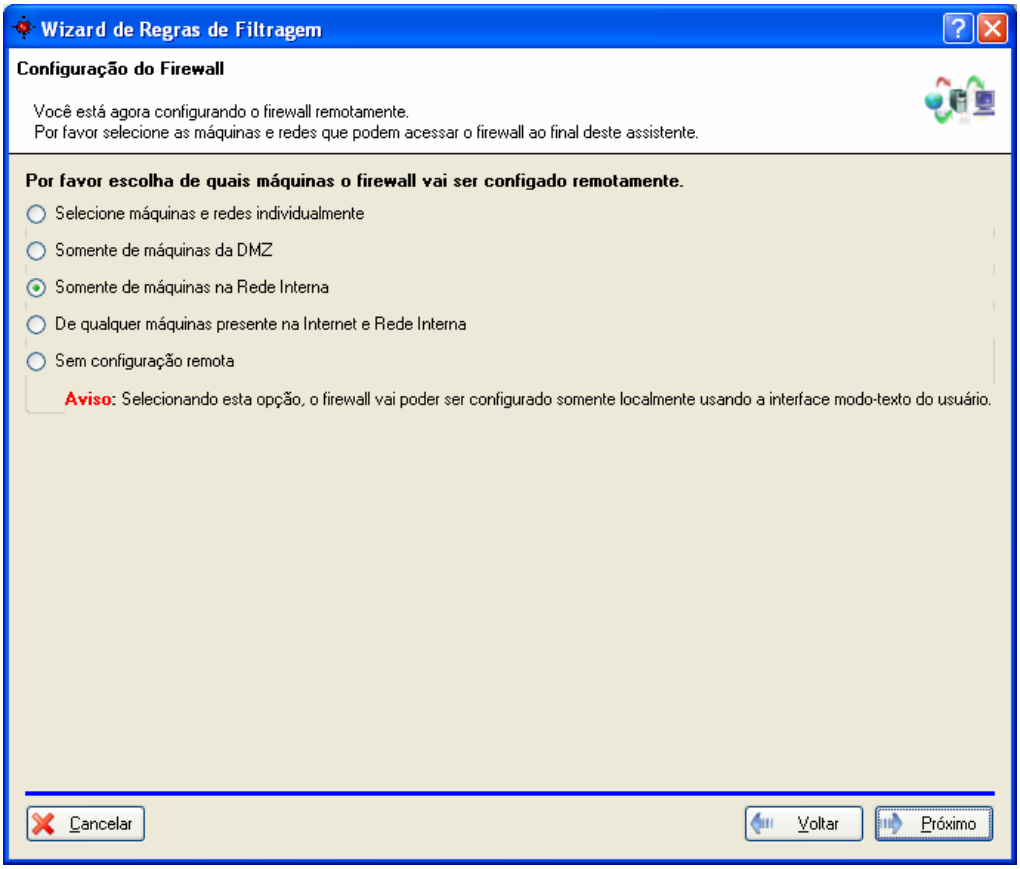
7 - Informação se a DMZ terá acesso irrestrito a Internet


Wizard de Regras de Filtragem
Acesso da DMZ a Internet
Escolha quais serviços na Internet os computadores da DMZ vão poder usar. Você pode especificá-los individualmente ou permitir o acesso total.
As máquinas na DMZ tem acesso irrestrito a Internet?
Sim
Não
Cancelar
Voltar
Próximo

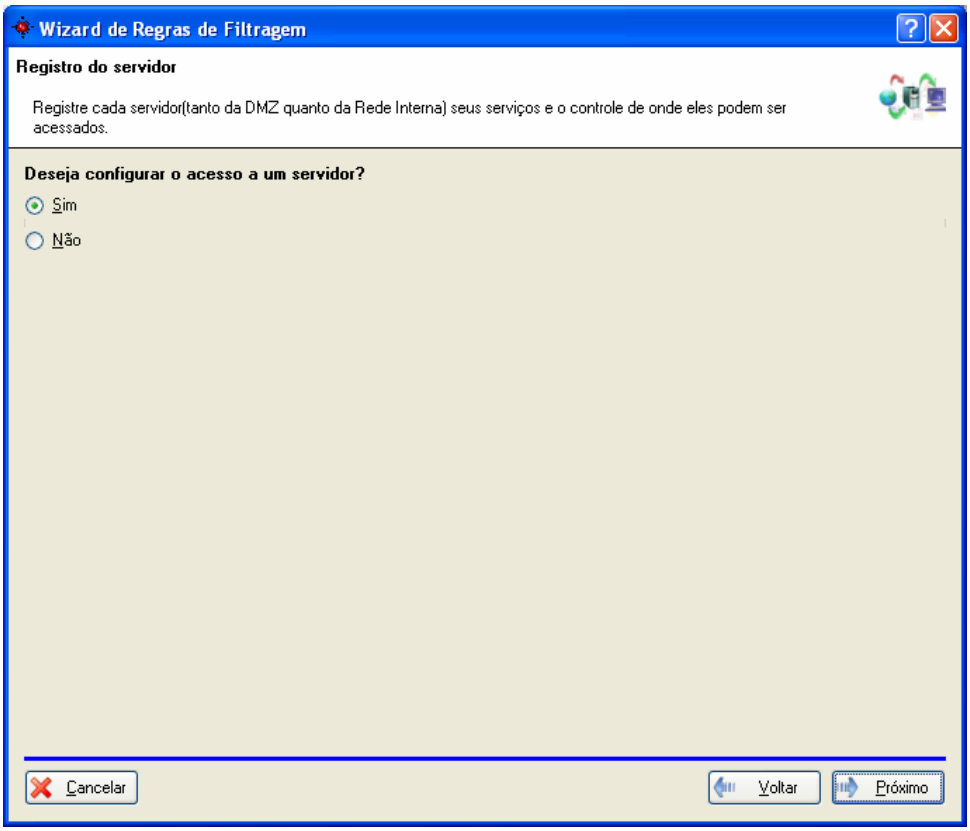
8 - Serviços a serem disponibilizados para a DMZ



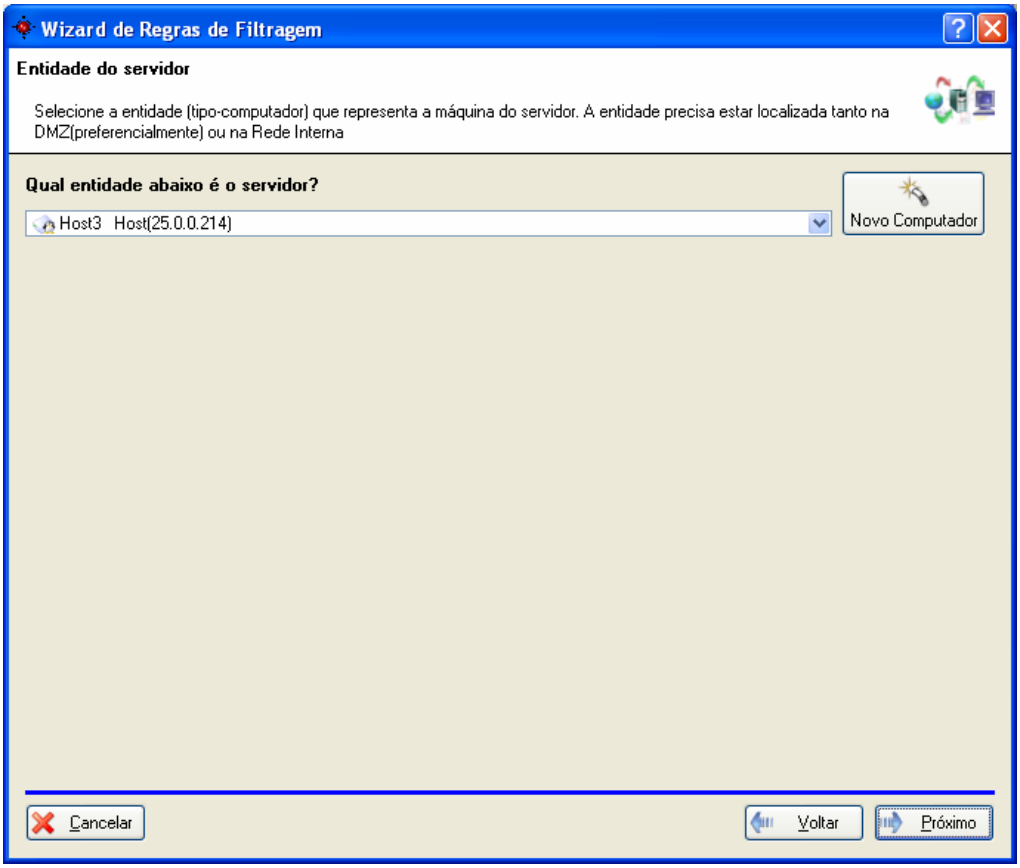
9 - Administração do Firewall. Informar quem terá acesso de administração ao mesmo.


Wizard de Regras de Filtragem
Configuração do Firewall
Você está agora configurando o firewall remotamente.
Por favor selecione as máquinas e redes que podem acessar o firewall ao final deste assistente.
Por favor escolha de quais máquinas o firewall vai ser configado remotamente.
Selecione máquinas e redes individualmente
Somente de máquinas da DMZ
Somente de máquinas na Rede Interna
De qualquer máquinas presente na Internet e Rede Interna
Sem configuração remota
Aviso: Selecionando esta opção, o firewall vai poder ser configurado somente localmente usando a interface modo-texto do usuário.
Cancelar
Voltar
Próximo

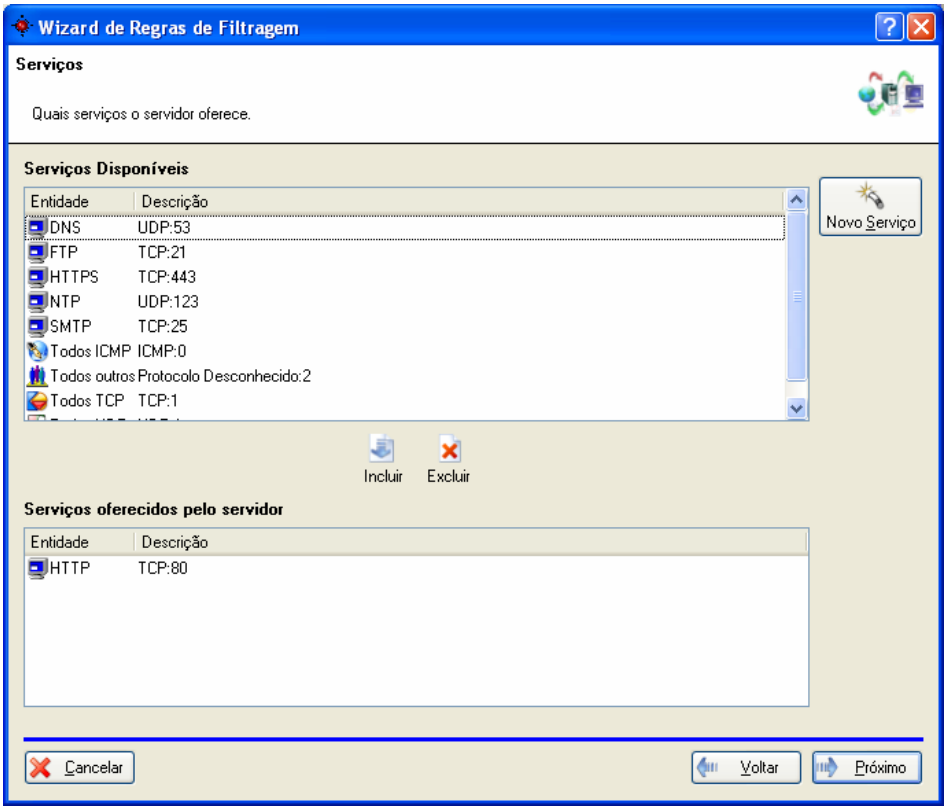
10- Registro individual de servidor para a DMZ


Wizard de Regras de Filtragem
Registro do servidor
Registre cada servidor(tanto da DMZ quanto da Rede Interna) seus serviços e o controle de onde eles podem ser acessados.
Deseja configurar o acesso a um servidor?
Sim
Não
Cancelar
Voltar
Próximo

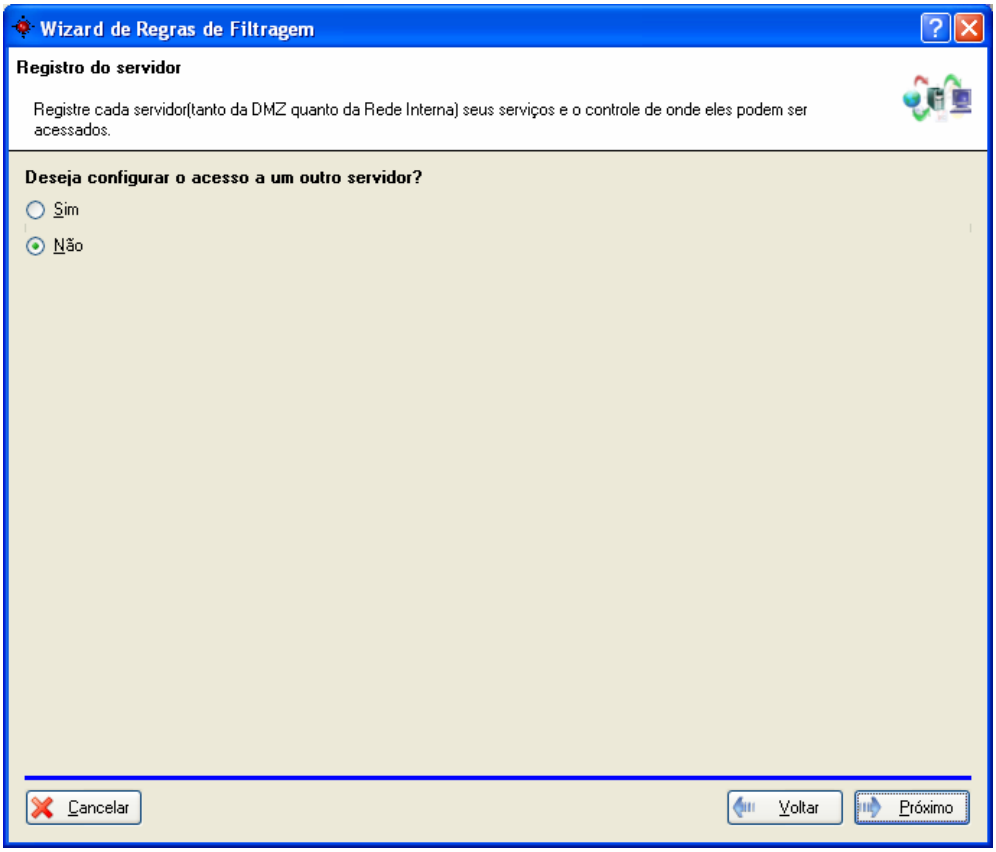
11 - Informação de servidor específico para a DMZ


Wizard de Regras de Filtragem
Entidade do servidor
Selecione a entidade (tipo-computador) que representa a máquina do servidor. A entidade precisa estar localizada tanto na DMZ(preferencialmente) ou na Rede Interna
Qual entidade abaixo é o servidor?
Host3 Host(25.0.0.214)
Novo Computador
Cancelar
Voltar
Próximo

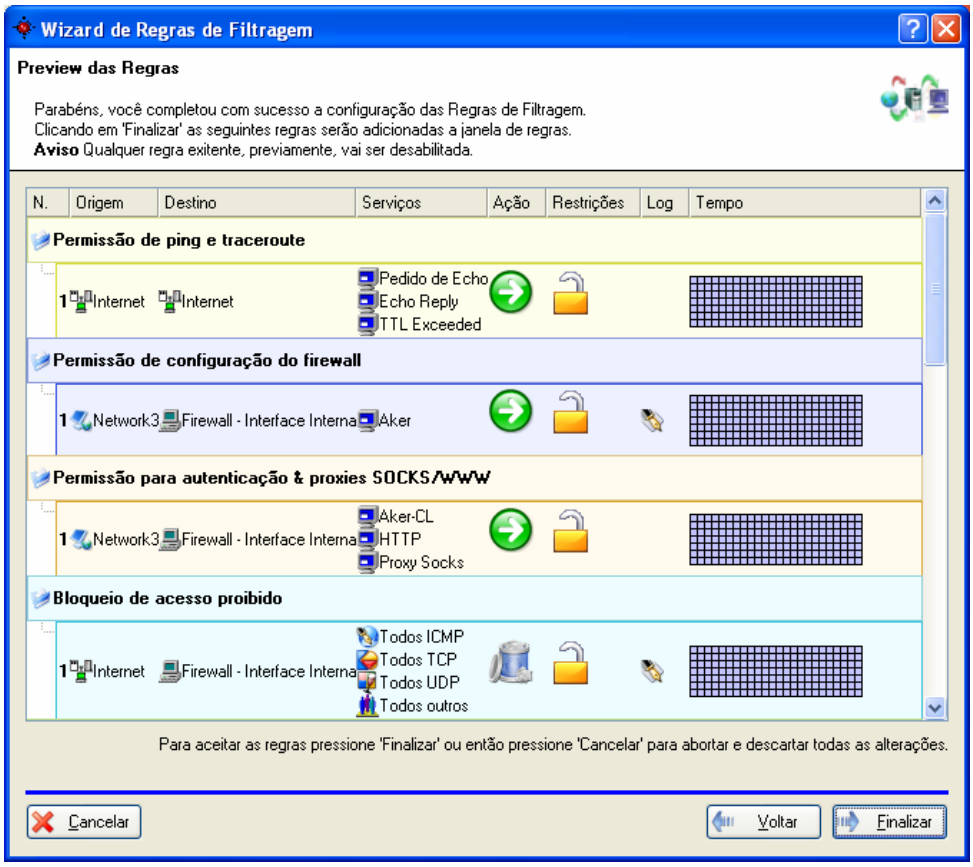
12 - Seleção dos serviços do servidor para a DMZ



13 - Pergunta se deseja configurar outro servidor.


Wizard de Regras de Filtragem
Registro do servidor
Registre cada servidor(tanto da DMZ quanto da Rede Interna) seus serviços e o controle de onde eles podem ser acessados.
Deseja configurar o acesso a um outro servidor?
Sim
Não
Cancelar
Voltar
Próximo

14 - Visualização final das regras de filtragem montada pelo assistente.



7-0 Configurando a conversão de endereços

Mostraremos aqui como configurar os parâmetros de conversão de endereços (NAT) de modo a possibilitar que sua rede interna trabalhe com endereços reservados, aumentando sua capacidade de endereçamento, escondendo as máquinas da rede interna e acessando a Internet, de forma totalmente transparente. Neste nova versão ttambém será possível realizar um balanceameto de carga das conexões de forma mais inteligente.

7-1 Planejando a instalação

O que é conversão de endereços?

Qualquer rede que vai se ligar à Internet necessita de um conjunto de endereços IP atribuídos por alguma autoridade designada para tal (no Brasil esta distribuição é de responsabilidade da Fapesp). Basicamente existem 3 conjuntos de endereços possíveis, os chamados classe A, que possibilitam 16.777.214 máquinas dentro da rede, os classe B, que possibilitam 65.533 máquinas e os classe C, que possibilitam 254 máquinas.

Devido ao grande crescimento apresentado pela Internet nos últimos anos, não existem mais endereços classe A e B disponíveis. Assim sendo, qualquer rede que venha a se conectar receberá um endereço classe C que permite o endereçamento de apenas 254 máquinas. Caso o número de máquinas seja maior do que isso, deve-se adquirir vários endereços classe C, dificultando o trabalho de administração, ou utilizar uma solução de conversão de endereços.

A conversão de endereços é uma tecnologia que permite que os endereços das máquinas da rede interna sejam distribuídos como se desejar, possivelmente usando endereços classe A, e mesmo assim todas as máquinas possam acessar de forma simultânea e transparente a Internet.

O seu funcionamento é simples: todas as vezes que uma máquina com um endereço reservado tenta acessar a Internet, o Firewall detecta e automaticamente traduz seu endereço para um endereço válido. Quando a máquina destino responde e envia dados para o endereço válido, o Firewall converte de volta este endereço para o reservado e repassa os dados para a máquina interna. Da forma que isso é feito, nem as máquinas clientes nem as máquinas servidoras sabem da existência de tal mecanismo.

Uma outra vantagem, além da apresentada acima, é que com a conversão de endereços todas as máquinas da sua rede interna ficam invisíveis para a rede externa, aumentando ainda mais o nível de segurança da instalação.

A conversão de endereços não é compatível com serviços que transmitem endereços IP ou portas como parte do protocolo. Os únicos serviços deste tipo suportados pelo Firewall Aker são o FTP , Real Audio e Real Vídeo.

Quais são minhas redes internas ?

As redes internas se constituem de todas as máquinas de uma ou mais sub-redes que estão sendo protegidas pelo Firewall Aker. Isto inclui todos os dispositivos internos à rede, como roteadores, switches, máquinas servidoras, máquinas clientes, etc. São os equipamentos que guardam informações importantes da sua rede, ou são peças chaves para seu funcionamento.

Quais são as minhas redes externas ?

As redes externas são formadas por todas as máquinas que não fazem parte da rede interna. Elas podem estar ou não sobre a responsabilidade administrativa de sua organização.

No caso de uma rede de uma organização se ligando à Internet, a rede externa seria toda a Internet.

Endereçando minhas redes internas

Apesar de tecnicamente possível, os endereços de suas redes internas não devem ser escolhidos a revelia. Existem alguns endereços reservados especificamente para este fim. Estes endereços não são e nunca serão atribuídos a nenhuma máquina ligada à Internet.

Os endereços reservados são:

De **10.0.0.0** à **10.255.255.255**, máscara 255.0.0.0 (classe A)
De **172.16.0.0** à **172.31.0.0**, máscara 255.255.0.0 (classe B)
De **192.168.0.0** à **192.168.255.255**, máscara 255.255.255.0 (classe C)

Tipos de conversão de endereços

Existem três tipos diferentes de conversão de endereços: 1-1, N-1 e 1-N. Cada um deles possui características distintas e normalmente são utilizados em conjunto para conseguir melhores resultados.

- 1-1

O tipo 1-1 é o mais intuitivo porém normalmente o menos útil. Ele consiste em fazer mapeamentos binários de um para um entre endereços reservados e endereços válidos. Desta forma, máquinas distintas teriam endereços convertidos distintos.
A grande limitação desta forma de operação é que não é possível se colocar um número de máquinas maior que o número de endereços válidos, uma vez que são sempre convertidos na base de um para um. Em compensação, ela permite que máquinas com endereços reservados possam ser acessadas externamente com endereços válidos.

- N-1

A conversão de N-1, como o nome já diz, possibilita que várias máquinas com endereços reservados utilizem um mesmo endereço válido. Para conseguir este objetivo, ela utiliza endereços IP em combinação com portas (no caso dos protocolos TCP e UDP) ou com números de seqüência (no caso de ICMP). Este mapeamento é feito dinamicamente pelo firewall, cada vez que uma nova conexão é estabelecida. Como existem 65535 portas ou números de seqüência distintos, é possível a existência de até 65535 conexões simultâneas ativas utilizando o mesmo endereço.
A única limitação desta tecnologia é que ela não permite que as máquinas internas sejam acessadas externamente. Todas as conexões devem ser iniciadas internamente.

- 1-N

Este tipo de conversão é também chamado de balanceamento de carga e possibilita que vários servidores sejam colocados atrás de um único endereço IP válido. Cada vez que uma uma nova conexão é aberta para esse endereço, ela é redirecionada para um dos servidores internos. A grande vantagem dessa tecnologia é possibilitar que serviços que demandam uma grande quantidade de recursos possam ser separados em várias máquinas e serem acessados de forma transparente, através de um único endereço. No caso de quedas de algumas dessas máquinas, as novas conexões são automaticamente repassadas para as máquinas que ainda estiverem no ar, implantando com isso mecanismo de tolerância a falhas.

Aplicações da conversão de endereços com o Firewall Aker

O Firewall Aker permite que qualquer tipo de conversão seja realizada, não se limitando apenas ao endereço válido da interface externa do firewall, mas sim dando total flexibilidade ao administrador em utilizar qualquer endereço dentro da rede, inclusive fazendo a conversão entre redes inválidas.

Suponhamos que uma determinada organização receba uma endereço classe C, com o formato A.B.C.0. Este endereço é um endereço válido que suporta no máximo 254 máquinas (os endereços A.B.C.0 e A.B.C.255 são reservados para fins específicos e não podem ser utilizados, sobrando os valores de A.B.C.1 a A.B.C.254). Suponha ainda que esta rede possui 1000 máquinas para serem conectadas. Em virtude da impossibilidade de se alocar todas as máquinas no endereço recebido, foi decidido pelo uso da conversão de endereços. Escolheu-se então um endereço reservado classe A para ser colocado nas máquinas da rede interna, o 10.x.x.x com máscara 255.0.0.0.

O Firewall Aker irá ficar na fronteira da Internet com a rede interna, que possui endereços reservados. Ele será o responsável pela conversão dos endereços reservados 10.x.x.x para os endereços válidos A.B.C.x. Desta forma, o firewall deverá possuir pelo menos dois endereços: um endereço válido, para que possa ser atingido pela Internet e um reservado, para que possa ser atingido pela rede interna. (na maioria das instalações, coloca-se duas ou mais placas de rede no firewall: uma para a rede externa e uma ou mais para a rede interna. Entretanto é possível, porém não recomendado, se fazer esta mesma configuração com apenas uma placa de rede, atribuindo um endereço válido e um reservado para a mesma placa)

Supondo que se escolha o endereço A.B.C.2 para o segmento válido e o 10.0.0.2 para o segmento reservado. Este endereço válido será utilizado pelo firewall para converter todas as conexões com origem na rede interna e destino na Internet. Externamente, todas as conexões serão vistas como se partissem dele.

Um outro exemplo seria a de uma organização que possua saídas para a Internet e três classes de endereços válidos, neste caso o administrador tem a possibilidade de distribuir a conversão de endereços entre essas três classes, obtendo muito mais flexibilidade na configuração.

Com a conversão de endereços funcionando, todas as máquinas internas conseguem acessar qualquer recurso da Internet transparentemente, com se elas próprias possuíssem endereços válidos. Porém, não é possível para nenhuma máquina externa iniciar uma conexão para qualquer máquina interna (devido ao fato delas não possuírem endereços válidos). Para resolver este problema, o Firewall Aker posssibilita a configuração de regras de conversão 1-1, o que permite simular endereços válidos para quaisquer endereços reservados.

Voltando para o caso da nossa hipotética organização, suponha que em sua rede exista um servidor WWW, com endereço 10.1.1.5, e que seja desejado que este servidor forneça informações para a rede interna bem como para a Internet. Neste caso, é necessário se escolher um endereço válido para que este possa ser utilizado pelos clientes externos para se conectarem a este servidor. Suponha que o endereço escolhido tenha sido o A.B.C.10. Deve-se então acrescentar uma regra de conversão 1-1, de modo a mapear o endereço A.B.C.10 para o endereço interno 10.1.1.5. A partir deste momento, todos os acessos para A.B.C.10 serão automaticamente remapeados pelo firewall para 10.1.1.5.

Os endereços válidos escolhidos para realizar a conversão de 1-1 não podem ser atribuídos a nenhuma máquina real. Desta forma, em nosso exemplo, é possível a configuração de até 253 servidores na sua rede interna passíveis de serem acessados externamente (um dos 254 endereços válidos já é usado para o firewall para converter o tráfego de todas as máquinas clientes).

O Firewall Aker utiliza a tecnologia de proxy-arp para possibilitar que os *servidores virtuais* sejam tratados pelas máquinas pertencentes à rede válida (por exemplo, o roteador externo), como se fossem máquinas reais.

Exemplos de configurações usando conversão de endereços

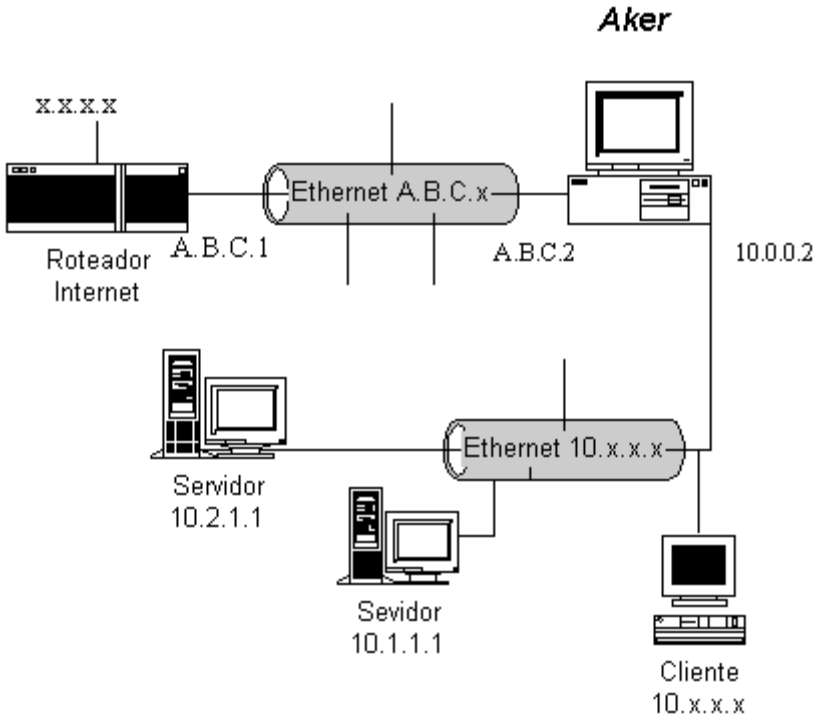
- **Se ligando à Internet com uma linha dedicada**

Equipamento: 1 roteador, 1 Firewall *Aker*, n clientes, 2 servidores na rede interna
Endereço válido: A.B.C.x, máscara da rede 255.255.255.0
Endereço reservado: 10.x.x.x máscara da rede 255.0.0.0
Endereço dos servidores: 10.1.1.1, 10.2.1.1
Endereço dos clientes: 10.x.x.x
Endereços do roteador: Rede válida A.B.C.1 , Internet :x.x.x.x
Configuração do Firewall Aker:

Endereços das placas: rede interna: 10.0.0.2, rede válida A.B.C.2
IP virtual para a conversão N-1: A.B.C.2
Rede privada: 10.0.0.0
Máscara da rede privada: 255.0.0.0

Regras de conversão 1-1:

A.B.C.10 - 10.1.1.1
A.B.C.30 - 10.2.1.1



Desenho do Exemplo 1

- **Interligando departamentos**

Neste exemplo, iremos mostrar como interligar departamentos de uma mesma empresa, utilizando um conversor de endereços entre estes departamentos.
Equipamento: 1 roteador, 3 Firewall *Aker*, n clientes, 4 servidores na rede interna
Endereço válido: A.B.C.x, máscara da rede 255.255.255.0
Endereço reservado: 10.x.x.x máscara da rede 255.255.0.0
Endereço reservado:172.16.x.x, máscara 255.255.0.0
Endereços da sub-rede 1:
10.1.x.x
Endereço do servidor: 10.1.1.1
Endereço dos clientes: 10.1.x.x
Endereços do roteador: Rede válida A.B.C.1 , Internet: x.x.x.x
Configuração do Firewall Aker:

Rede interna: 10.1.0.1, Rede válida A.B.C.2
IP virtual para a conversão N-1: A.B.C.2
Rede privada: 10.0.0.0
Máscara da rede privada: 255.0.0.0

Endereços da sub-rede 2:

Externamente: 10.1.0.2
Internamente:172.16.x.x

Endereço do servidor: 172.16.1.1
Endereço dos clientes: 172.16.x.x

Configuração do Firewall Aker:

Sub-Rede 2: 172.16.0.1, Sub-rede 1:10.1.0.2
IP Virtual para conversão N-1:10.1.0.2
Rede privada (2): 172.16.0.0
Máscara da rede privada: 255.255.0.0

Regras de conversão 1-1:

10.2.1.1 - 172.16.1.1

Endereços da sub-rede 3:

Externamente: 10.1.0.3
Internamente:172.16.x.x
Endereço do servidor: 172.16.1.1
Endereço dos clientes: 172.16.x.x

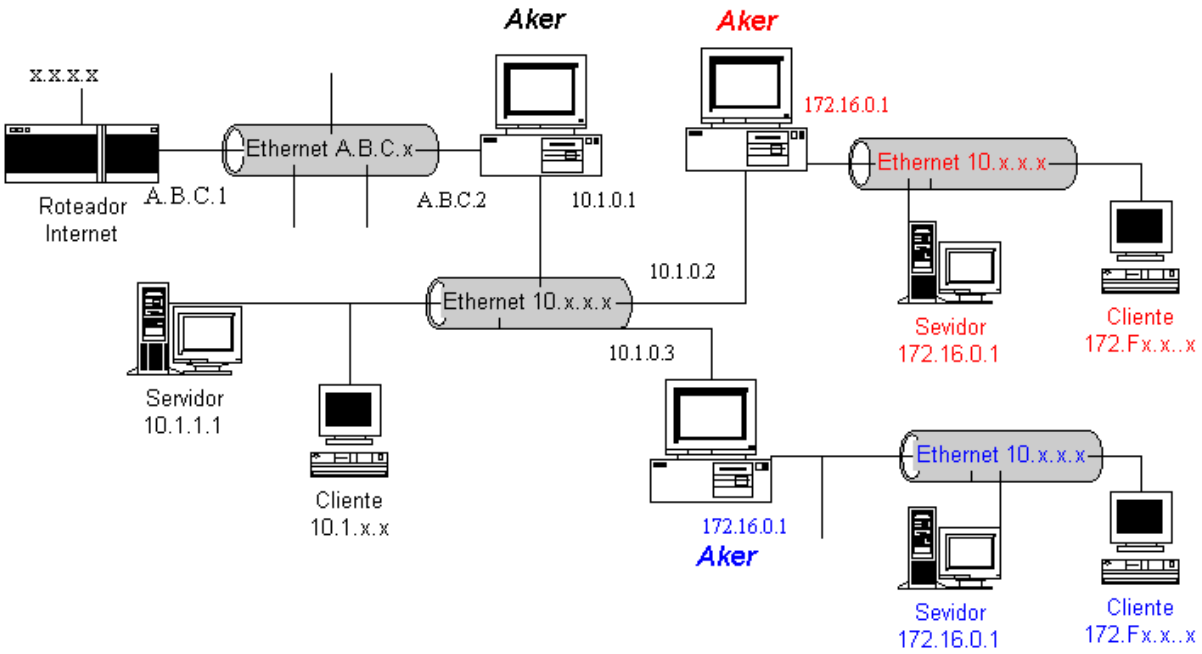
Configuração do Firewall Aker:

Sub-Rede 3: 172.16.0.1, Sub-rede 1:10.1.0.3
IP Virtual para conversão N-1:10.1.0.3
Rede privada (3): 172.16.0.0
Máscara da rede privada: 255.255.0.0

Regras de conversão 1-1:

10.3.1.1 - 172.16.1.1

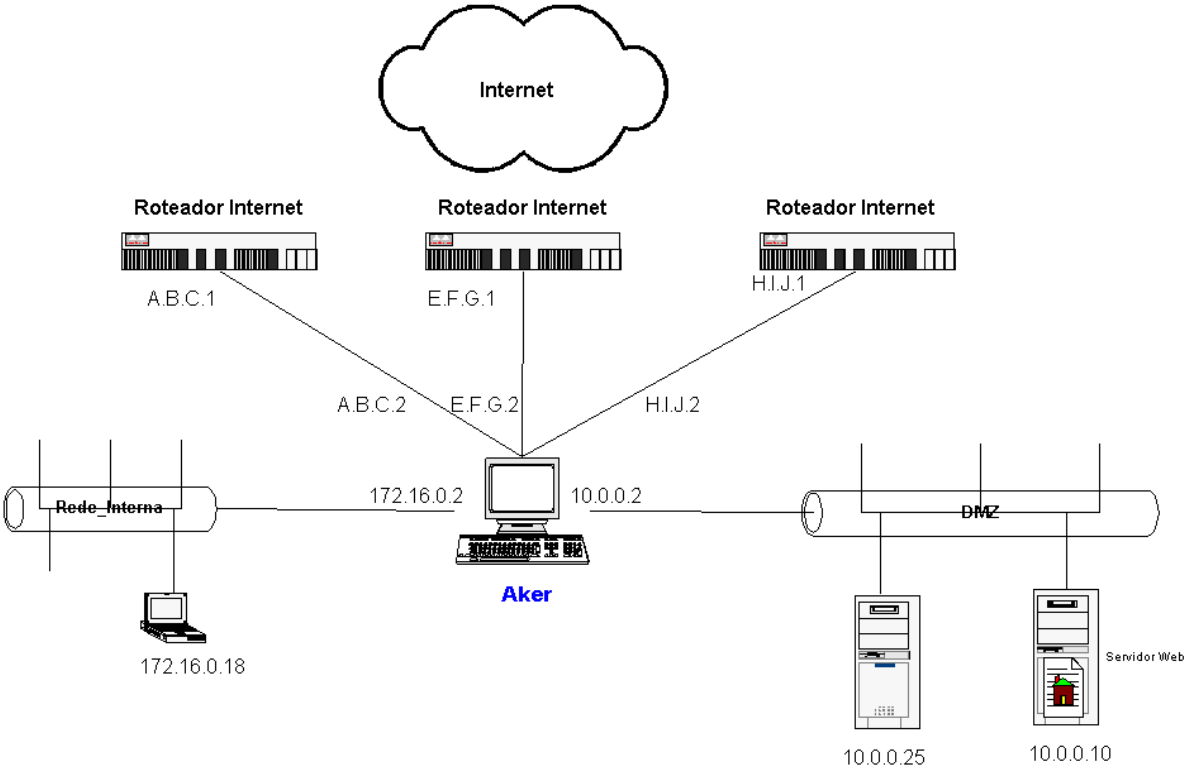
Na tabela de roteamento para este tipo de instalação devemos inserir rotas para as sub-redes 10.1.x.x, 10.2.x.x, 10.3.x.x.



Desenho do Exemplo 2

- **Múltiplas ligações com a Internet**

Neste exemplo, bem mais complexo, mostraremos como utilizar três ligações com a Internet e duas redes internas, utilizando o conversor de endereços entre elas.
Equipamento: 3 roteadores, 1 Firewall *Aker*, n clientes, 2 servidores na rede DMZ
Endereços válidos: A.B.C.x, D.E.F.x, G.H.I.x, todos com máscara de rede 255.255.255.0
Endereço reservado para a rede interna: 10.x.x.x máscara da rede 255.0.0.0
Endereço reservado para a DMZ:172.16.x.x, máscara 255.255.0.0
Endereços dos roteadores: Rede válida A.B.C.1, D.E.F.1, G.H.I.1 , Internet :x.x.x.x
Configuração do Firewall Aker:
Endereços das placas: Placa 1: 10.0.0.2, Placa 2: 172.16.0.2 , Placa 3: A.B.C.2, Placa 4: D.E.F.2, Placa 5: G.H.I.2
Redes privadas: 10.0.0.0 e 172.16.0.0
Máscara da redes privadas: 255.255.0.0
Servidores da DMZ
Servidor Web - 10.0.0.10
Servidor SMTP - 10.0.0.25
Regras de conversão de Endereços
1. Origem - 10.0.0.10 converte para A.B.C.10 quando for para a Internet
2. Origem - 10.0.0.25 converte para D.E.F.25 quando for para a Internet
3. Origem - 172.16.x.x converte para 10.0.0.4 quando for para rede 10.0.0.0
4. Origem - 172.16.x.x converte para D.E.F.25 quando for para Internet
5. Origem - 10.x.x.x converte para A.B.C.20 quando for para Internet



Desenho do Exemplo 3

Nesta nova versão do Firewall Aker é possível realizar um balanceamento dos links para realizar um aproveitamento mais otimizado dos links. O firewall agora possui mecanismos de verificação de ativação dos links, sendo possível dividir o tráfego de forma inteligente pelos links ou desviar totalmente o tráfego daquele que estiver fora do ar.

O administrador também poderá atribuir pesos às suas conexões ou seja as conexões mais rápidas poderão ter um peso maior do que as conexões mais lentas, desta forma o firewall dará preferência em enviar o tráfego para o link com maior peso.

Montando regras de conversão de endereços para o Firewall Aker

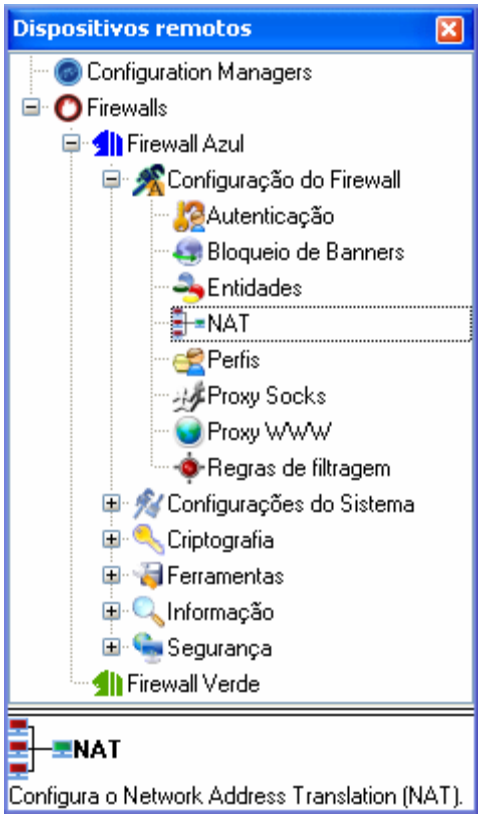
Configurar as regras de conversão de endereços no Firewall Aker é algo fácil em função de sua concepção inteligente. Toda a parte de endereços IP, máscaras, protocolos e portas é configurada nas entidades (para maiores informações, veja o capítulo intitulado Cadastrando Entidades). Devido a isso, ao configurar uma regra, não é necessário se preocupar com qual porta um determinado serviço utiliza ou qual o endereço IP de uma rede ou máquina. Tudo isso já foi previamente cadastrado. Para facilitar ainda mais, todos os serviços mais utilizados na Internet já vem previamente configurados de fábrica, sendo desnecessário perder tempo pesquisando os dados de cada um.

Basicamente, para cadastrar uma regra de conversão, deve-se especificar as entidades de origem e destino, tipo de conversão, interface virtual e serviço (se for o caso).

O funcionamento da conversão é simples: o firewall pesquisará uma a uma as regras definidas pelo administrador, na ordem especificada, até que o pacote se encaixe numa delas. A partir deste momento, ele executará o tipo de conversão associado à regra. Caso a pesquisa chegue ao final da lista e o pacote não se enquadre em nenhuma regra então este não será convertido.

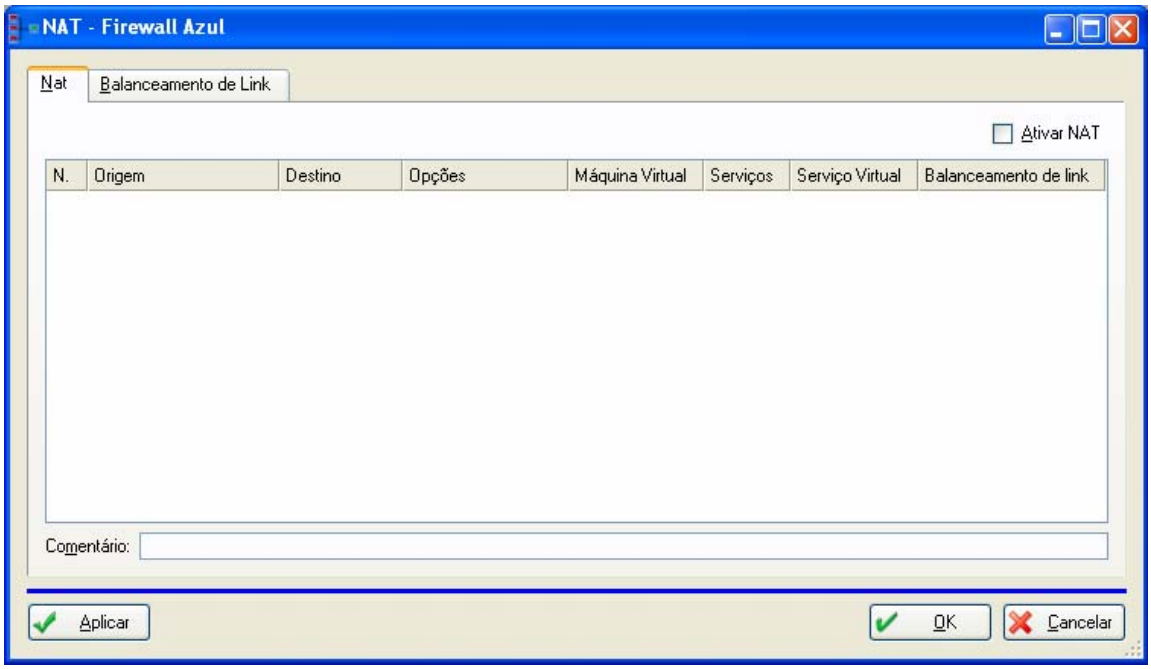
7-2 Utilizando a interface gráfica

Para ter acesso a janela de configuração da conversão de endereços, basta:



- Clicar no menu *Configuração do Firewall*
- Selecionar o item *NAT*

A janela de configuração da conversão de endereços (NAT)



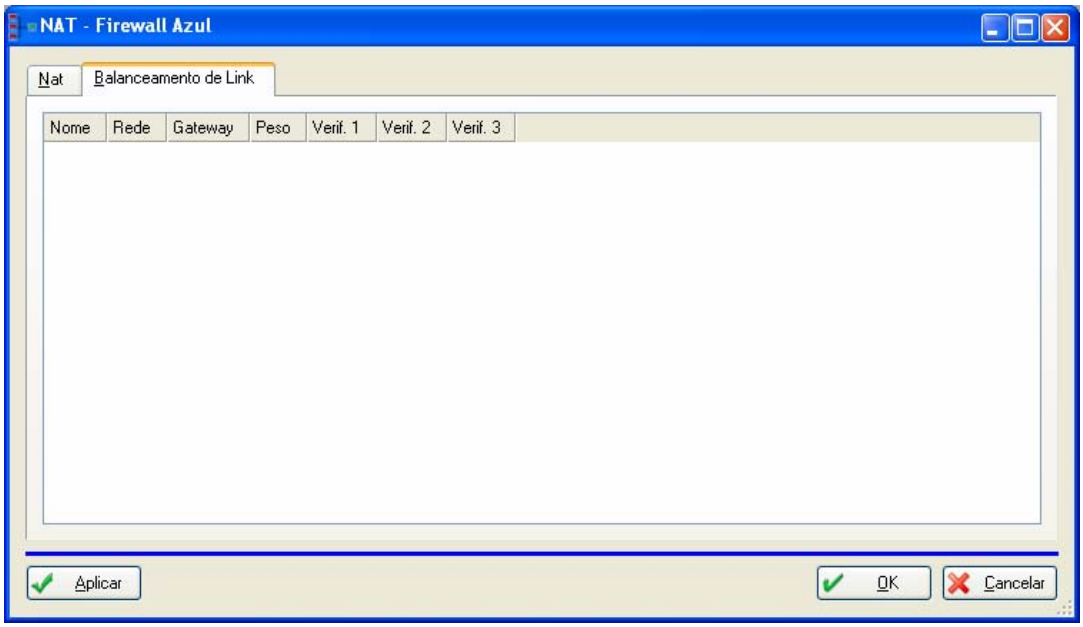
A janela de conversão de endereços contém todas as regras de conversão definidas no Firewall Aker. Cada regra será mostrada em uma linha separada, composta de diversas células. Caso uma regras esteja selecionada, ela será mostrada em uma cor diferente.

- O botão **OK** fará com que o conjunto de regras seja atualizado e passe a funcionar imediatamente.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta
- O botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.
- Existe uma barra para inclusão de comentários relativo a regra de conversão.

- A opção **Ativar NAT**, se estiver marcada, fará com que o firewall passe a converter os endereços de acordo com as regras cadastradas. Caso ela esteja desmarcada nenhum tipo de conversão de endereços será feita.

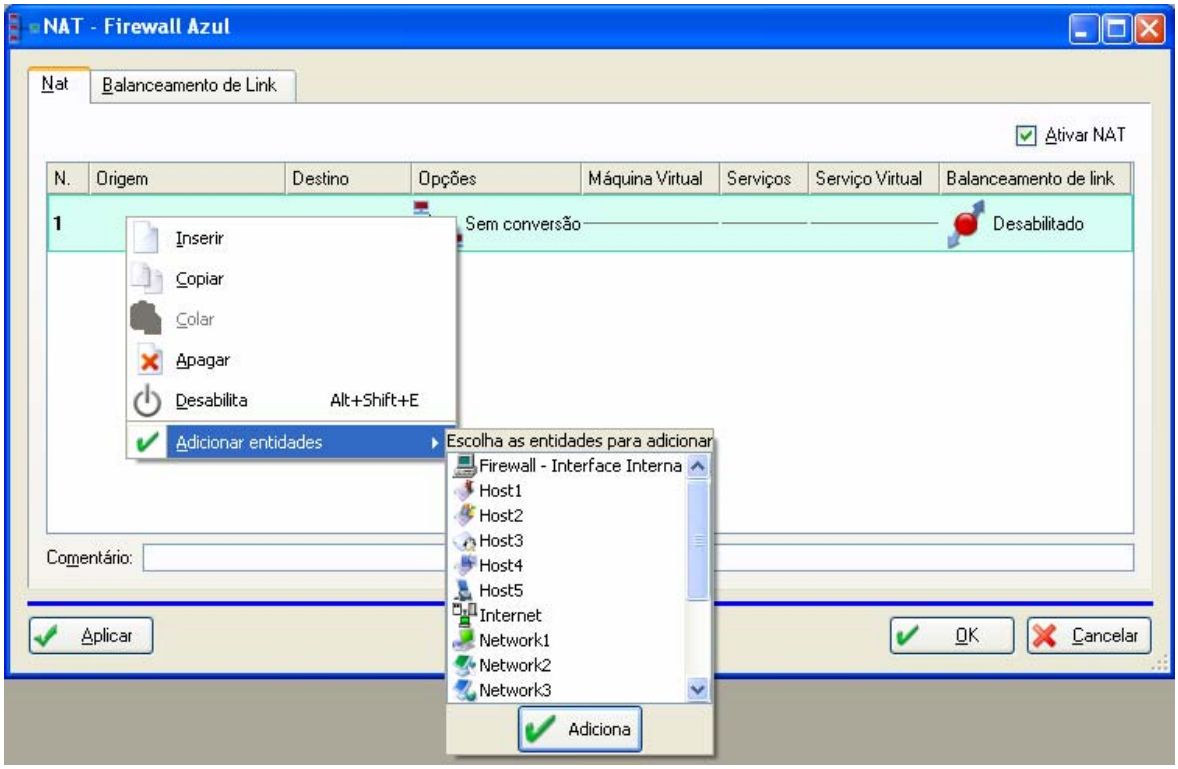
- A barra de rolagem do lado direito serve para visualizar as regras que não couberem na janela.
- Ao se clicar sobre uma regra e selecioná-la, se ela possuir um comentário, este aparecerá na parte inferior da janela.
- A posição da regra pode ser alterada clicando e arrastando com o mouse para a nova posição desejada.

A janela de configuração de Balanceamento de Link



- O botão **OK** fará com que o conjunto de regras seja atualizado e passe a funcionar imediatamente.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta
- O botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.

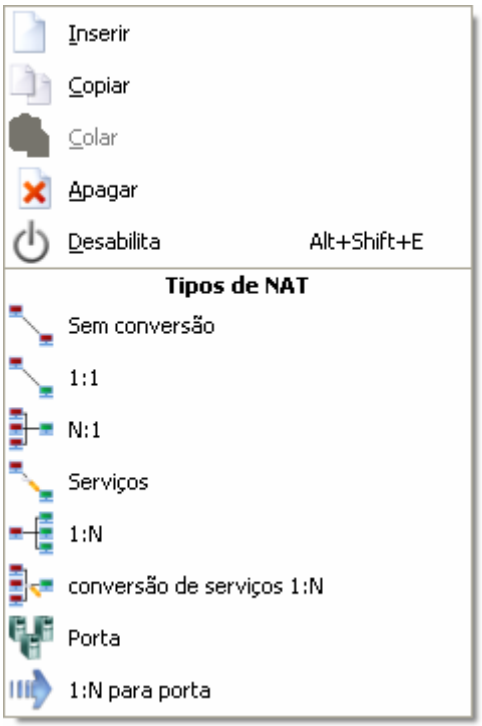
Para se executar qualquer operação sobre uma determinada regra, basta clicar com o botão direito do mouse sobre ela. Aparecerá o seguinte menu: (este menu será acionado sempre que se pressionar o botão direito, mesmo que não exista nenhuma regra selecionada. Neste caso, somente as opções *Incluir* e *Colar* estarão habilitadas).



- **Incluir:** Esta opção permite se incluir uma nova regra na lista. Se alguma regra estiver selecionada, a nova será inserida na posição da regra selecionada. Caso contrário, a nova regra será incluída no final da lista.
- **Apagar**: Esta opção remove da lista a regra selecionada.
- **Copiar:** Esta opção copia a regra selecionada para uma área temporária.
- **Colar:** Esta opção copia a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.
- **Enable/Disable:** Esta opção permite habilitar/desabilitar a regra selecionada, ou seja, ela permanecerá cadastrada contudo o Firewall se comportará como se a mesma não existisse (no caso do Disable) e prosseguirá a pesquisa na regra seguinte.
- **Adicionar entidades:** No ponto em que for feito o clique do mouse, será possível inserir a entidade no campo correspondente da regra de conversão. Apenas um certo número de entidades poderá ser visualizada, para escolher outra entidade faça a rolagem da janela na barra correspondente.

Dica: O método mais prático para o administrador montar sua regra de conversão será arrastando diretamente as entidades para dentro da regra.
Dica 2: A posição de cada regra pode ser alterada, bastando clicar e arrastar a mesma para a nova posição desejada, soltando em seguida. Observe que o cursor de indicação do mouse irá mudar para uma caixa pontilhada.
No caso de inclusão ou edição de regras, será mostrada a janela de propriedades, descrita na seção abaixo:

A janela de inclusão de regras de NAT



Tipo de NAT: Neste campo se define o tipo de conversão que a regra realizará. Ela possui as seguintes opções:

- **Sem Tradução**: Esta opção indica ao firewall que não deve haver conversão de endereços quando qualquer uma das máquinas pertencentes às *Entidades Origem* forem acessar qualquer uma das máquinas pertencentes às *Entidades Destino* e vice-versa.

- **Conversão 1-1**: Esta opção indica ao firewall que quando a máquina listada nas *Entidades Origem* for acessar acessar qualquer uma das máquinas pertencentes às *Entidades Destino* ela terá seu endereço convertido para o endereço da *Entidade Virtual*. Todas as vezes que uma máquina pertencente às *Entidades Destino* acessar o endereco da *Entidade Virtual*, esse ultimo será automaticamente convertido para o endereço real, definido pela entidade presente nas *Entidades Origem*. Este tipo de conversão é útil para possibilitar o acesso externo a servidores internos.

Nas *Entidades Origem* deve se colocar uma entidade com o endereço real (interno, reservado) da máquina para a qual se fará conversão de 1-1. Na *Entidade Virtual* deve-se colocar uma entidade com o endereço para o qual o endereço interno será convertido (endereço válido) e que será acessado pelas máquinas externas.

- **Conversão N-1**: Esta opção indica ao firewall que quando qualquer máquina listada nas *Entidades Origem* for acessar acessar qualquer uma das máquinas pertencentes às *Entidades Destino* ela terá seu endereço convertido para o endereço da *Entidade Virtual*. Este tipo de conversão é útil para possibilitar que um grande número de máquinas utilize apenas um endereço IP válido para se comunicar através da Internet, entretanto ela não permite com que máquinas externas (listadas nas *Entidades Destino*) iniciem qualquer comunicação com as máquinas internas (listadas nas *Entidades Origem*).

Quando o módulo de Cluster Cooperativo estiver funcionado na conversão de N-1 o IP da entidade virtual não pode ser nenhum dos atribuídos as interfaces do firewall.

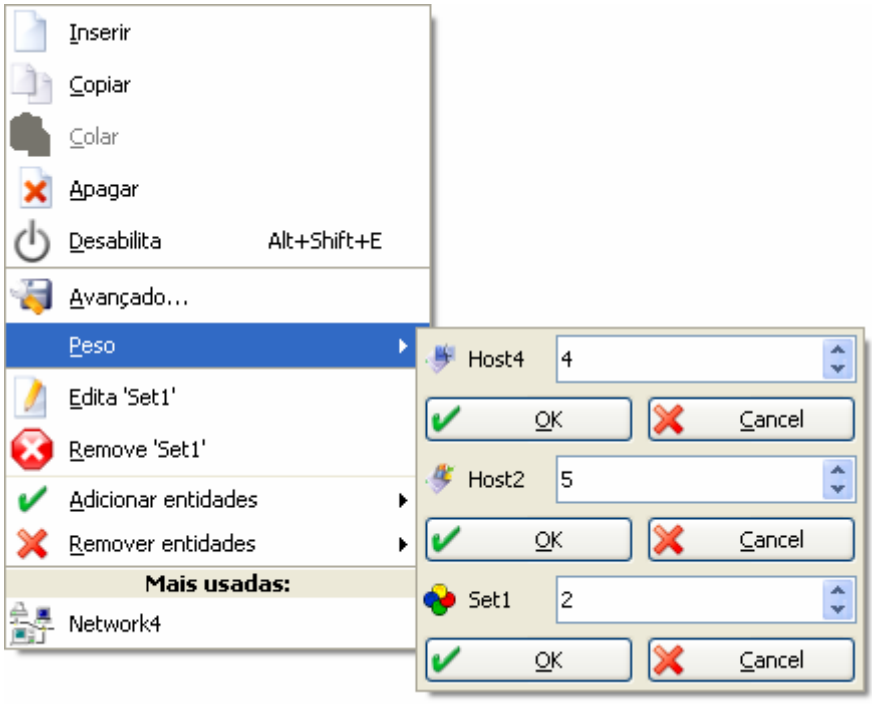
- **Conversão de Serviços**: Esta opção é útil para redes que dispõem de apenas um endereço IP e necessitam disponibilizar serviços para a Internet. Ela possibilita que determinados serviços, ao serem acessados no firewall, sejam redirecionados para máquinas internas.

No campo *Entidades Origem*, deve-se colocar o endereço IP interno (real) da máquina para a qual os serviços serão redirecionados. No campo *Entidades Destino*, deve-se colocar as máquinas que irão acessar os serviços externamente. No campo *Serviços*, deve-se escolher todos os serviços que serão redirecionados para a máquina presente em *Entidades Origem* quando uma máquina presente nas *Entidades Destino* acessá-los no endereço IP da *Entidade Virtual*.

Quando o módulo de Cluster Cooperativo estiver funcionado não é possível a conversão de serviços.

- **Conversão 1-N**: Esta opção é utilizada para se fazer balanceamento de carga, ou seja, possibilitar que várias máquinas respondam como se fossem uma única.

No campo *Entidades Origem* deve-se colocar a lista de máquinas que farão parte do balanceamento e que passarão a responder como se fossem uma única. No campo *Entidades Destino*, deve-se colocar as máquinas que irão acessar as máquinas internas pelo endereço especificado na entidade presente no campo *Entidade Virtual*.



Nesse tipo de conversão, as máquinas pertencentes ao campo *Entidade Origem* podem ter pesos diferentes, ou seja, caso uma máquina tenha peso 1 e outra peso 2, então significa que de cada 3 conexões, uma será redirecionada para a primeira máquina e duas para a segunda.

- **Conversão de Serviços 1-N**: Esta opção é utilizada para se fazer balanceamento de carga para determinados serviços, ou seja, possibilitar que várias máquinas respondam a requisições destes serviços como se fossem uma única.

No campo *Entidades Origem* deve-se colocar a lista de máquinas que farão parte do balanceamento e que passarão a responder como se fossem uma única. No campo *Entidades Destino*, deve-se colocar as máquinas que irão acessar as máquinas internas pelo endereço especificado na entidade presente no campo *Entidade Virtual*. No campo *Serviços*, deve-se escolher todos os serviços que farão parte do balanceamento.

Nesse tipo de conversão, as máquinas pertencentes ao campo *Entidade Origem* podem ter pesos diferentes, ou seja, caso uma máquina tenha peso 1 e outra peso 2, então significa que de cada 3 conexões, uma será redirecionada para a primeira máquina e duas para a segunda.

Quando o módulo de Cluster Cooperativo estiver funcionado não é possível a conversão de serviços.

Entidade virtual: Neste campo deve-se configurar a entidade para a qual os endereços internos serão convertidos ou para o qual as requisições externas devem ser direcionadas. A entidade virtual deverá sempre ser uma entidade do tipo máquina.

Entidade Origem: Neste campo especifica-se a lista de todas as entidades cujos endereços serão convertidos para o endereço da *Entidade Virtual*, descrita acima. A conversão 1-1 ou conversão de serviços permitem que apenas uma entidade seja selecionada para este campo e esta entidade deve ser do tipo máquina.

Caso se esteja utilizando Conversão 1-N ou Conversão de Serviços 1-N, então cada máquina pertencente a esse campo terá um pesso associado a ela, mostrado entre parânteses, à direita do nome da entidade. Para se alterar o peso de uma determinada máquina, ou seja, fazer com que ela receba mais conexões que as demais, basta se clicar com o botão direito sobre o nome da entidade, na lista da direita, selecionar a opção **Alterar peso** e escolher o novo valor.

O campo Entidade Origem deve sempre conter os endereços internos (reservados ou não válidos) das máquinas participantes da conversão, independentemente de seu tipo.

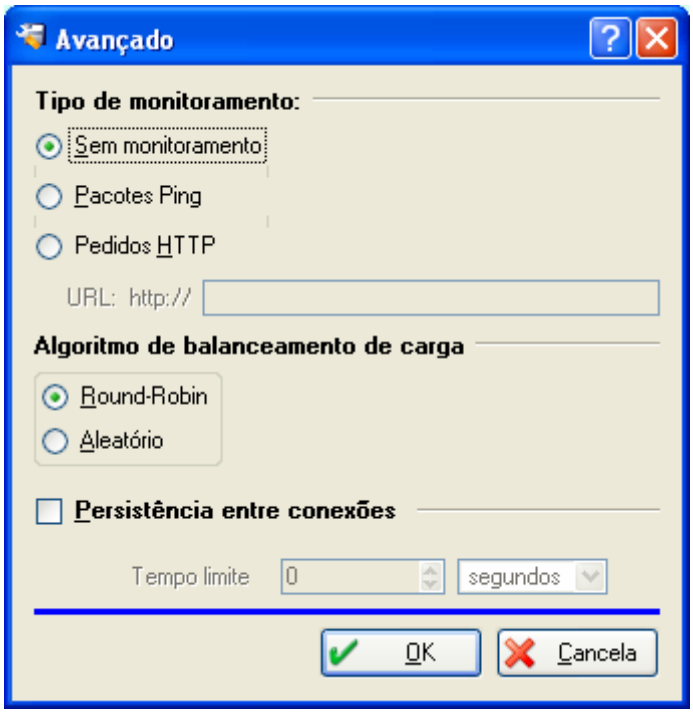
Entidade Destino: Este campo serve para se especificar as entidades para as quais a conversão de endereços será efetuada (no caso da conversão N-1) ou as máquinas que acessarão as máquinas internas através do endereço contido no campo *Entidade Virtual* (para os demais tipos de conversão). Criando-se várias regras com valores distinos nesse campo faz-se com que uma mesma máquina tenha seu endereço convertido para endereços distindos dependendo do destino da comunicação.

O valor mais comum para esse campo é a especificação da entidade *Internet* como destino. Isso fará com que a conversão de endereços selecionada na regra seja efetuada para todas as máquinas externas.

Serviços: Este campo define quais os serviços que farão parte da regra, quando for utilizada o tipo de conversão de Serviços ou 1-N com Serviços. A janela ficará desabilitada para os demais tipos de conversão.

Comentário: Reservado para se colocar uma descrição sobre a regra. Muito útil na documentação e manutenção das informações sobre sua utilidade.

O botão **Avançado**, que somente estará habilitado quando se selecionar conversão de endereços 1-N ou Conversão de serviços 1-N, permite que se configure os parâmetros do monitoramento que será realizado pelo firewall a fim de detectar se as máquinas participantes do balanceamento estão no ar ou não e como o balanceamento será realizado. Ao ser clicado, a seguinte janela será mostrada:



O campo **Tipo de monitoramento**, permite que se defina o método utilizado pelo firewall para verificar se as máquinas participantes do balanceamento (máquinas definidas no campo *Entidades Origem*) estão no ar. Ela consiste das seguintes opções:
Sem monitoramento: Se essa opção for selecionada, o firewall não monitorará as máquinas e assumirá que elas estão sempre ativas.

Pacotes Ping: Se essa opção for selecionada, o firewall monitorará as máquinas através de pacotes ICMP de *Echo Request* e *Echo Reply* (que também são utilizados pelo comando PING, daí o nome dessa opção).

Requisições HTTP: Se essa opção for selecionada, o firewall monitorará as máquinas através de requisições HTTP. Nesse caso, é necessário se especificar a URL (sem o prefixo http://) que o firewall tenterá acessar em cada máquina para verificar se ela está ativa ou não.

Algoritmo de balanceamento de carga: Esse campo permite que se defina o método utilizado para balancear as requisições entre as máquinas presentes no campo *Entidades Origem*. Ele consiste das seguintes opções:
Round-Robin: Se essa opção for selecionada, o firewall distribuirá seqüencialmente as requisições para as máquinas participantes do balanceamento, uma a uma. Caso as máquinas tenham pesos diferentes, primeiro será distribuída uma conexão para cada máquina, a seguir uma conexão para cada máquina que rebeceu um número de conexões menor que seu peso e assim sucessivamente. Quanto todas as máquinas receberem o número de conexões equivalente a seu peso, o algoritmo se inicia.

Randômico: Se essa opção for selecionada, o firewall distribuirá as conexões de forma randômica entre as máquinas, ou seja, a probabilidade de uma conexão ser redirecionada para uma determinada máquina é igual a razão entre seu peso e o peso total de todas as máquinas.

Persistência de Sessão: Esse campo permite que se defina o tempo de persistência da sessão em protocolos ou aplicativos que utilizem mais de uma conexão em tempos diferentes, ou seja, o tempo máximo de espera por uma nova conexão após o término da primeira. Neste intervalo de tempo as novas conexões serão direcionadas pelo firewall ao mesmo servidor.

Observações sobre a montagem das regras

É altamente recomendável que as regras de conversão sejam colocadas na seguinte ordem:

1. Regras de Não Conversão
2. Regras de Conversão de Serviços
3. Regras de Conversão 1-1
4. Regras de Conversão de Serviços 1-N
5. Regras de Conversão 1-N
6. Regras de Conversão N-1

É necessário a inclusão de uma regra de Não Conversão com origem nas redes internas e destino nas próprias redes internas caso se pretenda administrar o firewall por uma máquina interna que participará de qualquer tipo de conversão. Essa regra deverá estar antes das demais regras de conversão.

Exemplos - Cenário 1 - Conversão de Endereços

Suponha que uma empresa possua as máquinas e serviços abaixo e deseja implementar a conversão de endereços. A empresa possui uma conexão dedicada com a Internet e seu provedor distribuiu uma faixa de endereços IP válidos na Internet de 200.120.210.0 até 200.120.210.63.

Na regra 1 colocamos as redes internas da empresa (DMZ e Interna) em não tradução. Está regra possibilita que caso alguma máquina interna da rede for administrar o firewall o seu endereço não é convertido e a administração seja possível. Estaria também correto em especificar as máquinas que são administradoras (Entidade Origem) e a interface por onde iremos administrar o firewall (Entidade de Destino) com a opção de "Sem tradução".

Na regra 2 o servidor **server1** fará uma conversão de 1:1 para o endereço 200.120.210.15, ou seja caso alguém da Internet procure pelo IP 200.120.210.15 será enviado para o servidor server1 (IP 10.20.0.50). Do mesmo modo caso o servidor server1 originar conexão para Internet o seu IP será 200.120.210.15.

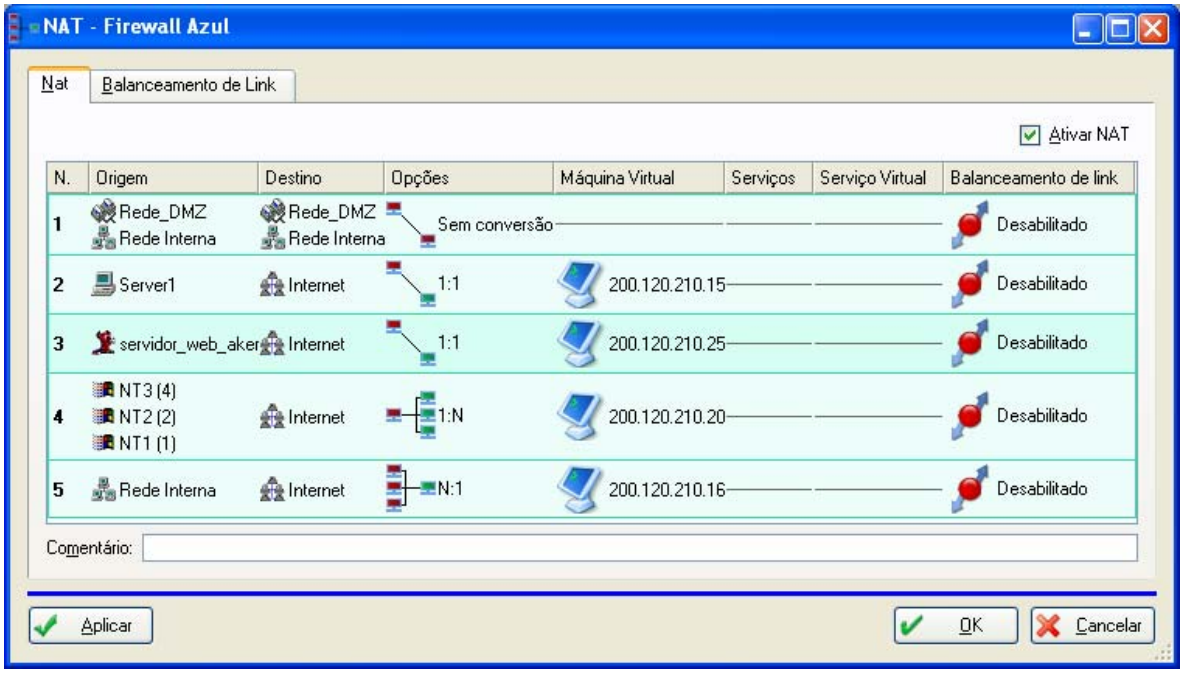
A regra 3 por analogia e identica a regra 2, o servidor servidor_web_aker fará conversão de 1:1 para o endereço 200.120.210.25.

A regra 4 é o exemplo de balanceamento de carga. Alguém da Internet procurando pela máquina 200.120.210.20 será enviado para o NT3, NT2 ou NT1. Isto dependerá do cálculo a ser realizado pelo firewall. No caso abaixo os pesos são diferentes, portanto a máquina NT3 que possui o peso 4 é a que receberá a maior quantidade de conexões.

Caso as máquinas NT tenham de originar conexões para Internet, elas também terão seus endereços convertidos para 200.120.210.20.

A regra 5 é de conversão de N:1, ou seja qualquer máquina da Rede_Interna (10.20.0.0 com máscara 255.255.255.0) terá o seu endereço convertido para 200.120.210.16 quando as mesmas originarem conexão para a Internet. No entanto a recíproca **não é verdadeira**, caso alguém da Internet venha procurando conexão para o IP 200.120.210.16 o firewall não enviará para nenhuma máquina da rede interna e irá descartar os pacotes para esta conexão, pois o mesmo não sabe para qual máquina enviar a requisição.

Cabe-se ressaltar que a ordem das regras é de extrema importância. Vamos supor que a **regra 2** seja movida para a **última posição**. Neste caso alguém que viesse procurando pela máquina **200.120.210.15** seria enviado para o **server1**, entretanto quando o **server1** fosse originar uma conexão para a Internet o mesmo teria seu endereço convertido para **200.120.210.16** pois a regra da antiga posição 5 é que iria atender primeiro a conversão.



Exemplos - Cenário 2 - Conversão de Serviços

Suponha agora que a empresa não possua uma faixa de endereços IP da Internet e sim um **Único** IP válido. Neste caso é conveniente que se faça a conversão de serviços. Com este tipo de configuração poderá ser feito um aproveitamento deste único IP para diversos tipos de serviços. No caso o IP é o 200.120.210.15.

A regra 1 foi colocada pelos mesmos motivos citados no cenário anterior.

Na regra 2 temos que alguém da Internet esteja procurando pela máquina 200.120.210.15 e na porta do servidor ftp (21/TCP). Neste caso o firewall irá enviar a conexão para a máquina server1

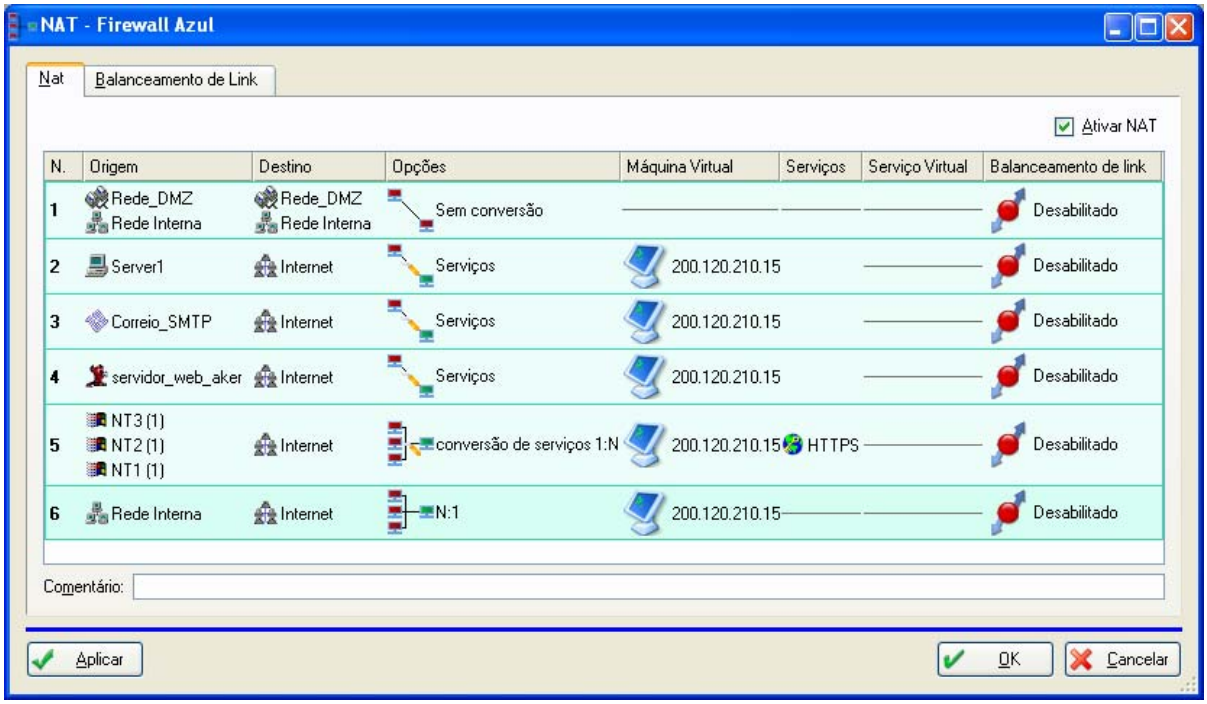
Na regra 3 alguém da Internet está procurando pela mesma máquina 200.120.210.15 porém na porta do smtp (25/TCP). O firewall irá mandar esta conexão para o endereço da entidade Correio_SMTP.

Já a regra 4 possibilita que o servidor web da empresa seja acessado pela porta http (80/TCP).

A regra 5 é um exemplo do balanceamento de carga utilizando uma porta de serviço. Neste caso alguém da Internet está procurando acesso ao IP 200.120.210.15 para o serviço web seguro (443/TCP), sendo que há três servidores para atender a requisição, no caso NT1, NT2 e NT3. Os princípios para atender estas conexões são os mesmos já explicados no cenário anterior.

Finalizando, a regra 6 permite que qualquer outra máquina origine conexão para Internet, no caso sendo visualizado o IP 200.120.210.15 no destino.

Apesar de ser possível utilizar a conversão de serviços no caso do cenário 1, a Aker recomenda que esta configuração seja utilizada no caso da empresa possuir somente um único endereço IP válido para Internet.


NAT - Firewall Azul
Nat
Balanceamento de Link
Ativar NAT
N.
Origem
Destino
Opções
Máquina Virtual
Serviços
Serviço Virtual
Balanceamento de link
1 Rede_DMZ Rede Interna | Rede_DMZ Rede Interna | Sem conversão | Desabilitado
2 Server1 | Internet | Serviços | 200.120.210.15 | Desabilitado
3 Correio_SMTP | Internet | Serviços | 200.120.210.15 | Desabilitado
4 servidor_web_aker | Internet | Serviços | 200.120.210.15 | Desabilitado
5 NT3 (1) NT2 (1) NT1 (1) | Internet | conversão de serviços 1:N | 200.120.210.15 | HTTPS | Desabilitado
6 Rede Interna | Internet | N:1 | 200.120.210.15 | Desabilitado
Comentário:
Aplicar
OK
Cancelar

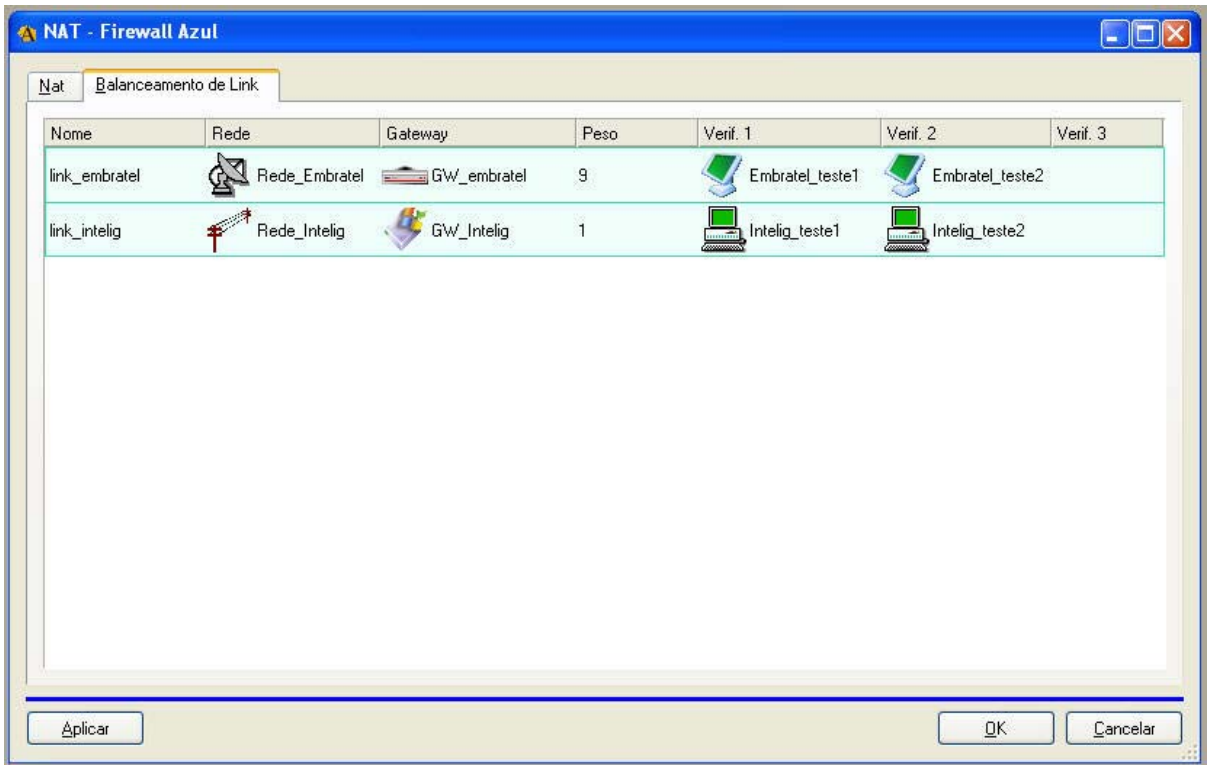
Exemplos - Cenário 3 - Balanceamento de Link

Neste cenário será descrito como se realizada o balanceamento de links. Suponha que a empresa possua dois prestadores de conexão IP para Internet, por exemplo, Embratel e Intelig. No caso cada operadora forneceu sua faixa de endereço IP para a empresa.

Primeira Fase - Montagem do Balanceamento

O administrador do firewal então irá realizar o cadastramento e informar as seguintes entidades e campos:

- **Nome:** Informe um nome para representar o link da operadora;
- **Rede:** Cadastre a rede que a operadora forneceu;
- **Gateway:** O IP do roteador da operadora deve ser informado (neste caso o firewall fará uma crítica para verificar se o gateway realmente pertence a rede da operadora);
- **Peso:** Um valor a ser atribuído ao link, no caso peso maiores pressupõe links mais rápidos.
- **Verif. 1:** Cadastre uma entidade que tenha certeza que esteja logo a seguir do roteador da operadora, de preferência dentro de um ou dois saltos de seu roteador. Esta entidade será utilizada pelo firewall para determinar se o link está no ar ou não. Pode ser cadastrado um servidor DNS da operadora ou mesmo roteadores próximos.
- **Verif 2 e Verif. 3 :** Entidades de verificação também utilizadas pelo firewall. Não é mandatório que estejam cadastrados as três entidades de verificação, contudo quanto mais melhor para o sistema de verificação do firewall.



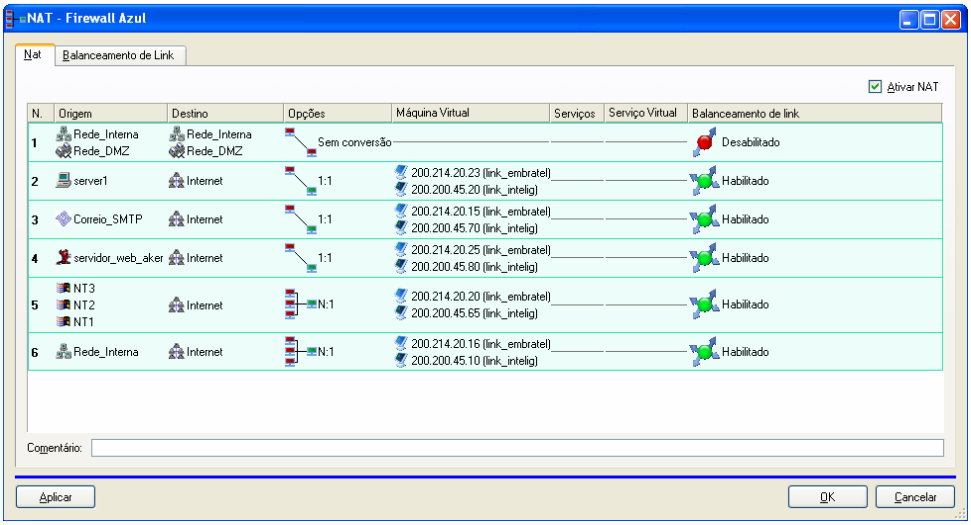
Segunda Fase - Montagem das Regras de NAT

A segunda fase da montagem é bem simples, bastando colocar em cada regra de conversão duas ou mais entidades virtuais, uma com endereço de cada prestador de serviço.

Não esqueça de habilitar na coluna *Balanceamento de links* o ícone correspondente para que o serviço possa ser realizado pelo firewall. Cabe ressaltar que o firewall também

realizará uma crítica para determinar se realmente a Entidade Virtual pertence a um link previamente cadastrado.

Uma limitação desta implementação é quanto a origem da conexão pela Internet. Os DNS devem ter entradas duplas de IP e devem trabalhar em modo Round-Robin. O problema está quando um link de determinada operadora cai, o firewall não tem como desviar as conexões que são originadas pela Internet. Para contornar este problema o administrador poderia utilizar de scripts para remover do DNS o IP da operadora que esteja fora do ar, pois o firewall passa para o log de eventos esta informação.



7-3 Utilizando a interface texto

A interface texto de configuração da conversão de endereços é relativamente simples e tem as mesmas capacidades da interface gráfica, exceto pelo fato de não ser possível se configurar os parâmetros de monitoramento.

Localização do programa: /etc/firewall/fwnat

Sintaxe:

```
Firewall Aker - Versao 5.1
fwnat - Configura regras de conversao de enderecos (NAT)
Uso: fwnat [ajuda | mostra | ativa | desativa]
     fwnat [habilita | desabilita | remove] <pos>
     fwnat inclui <pos> 1-1 <origem> <destino> [ <entidade virtual> |
                  -bal <ev_1> <ev_2> ... ]
     fwnat inclui <pos> n-1 <origem> <destino> [ <entidade virtual> |
                  -bal <ev_1> <ev_2> ... ]
     fwnat inclui <pos> servicos <origem> <destino> [ <entidade
virtual> |
                  -bal <ev_1> <ev_2> ... ] <servico1>...<servico2>
     fwnat inclui <pos> portas <origem> <destino> [ <entidade virtual>
|
                  -bal <ev_1> <ev_2> ... ] <servico> <servico virtual>
     fwnat inclui <pos> sem_conversao <origem> <destino>
     fwnat inclui <pos> 1-n <origem1>...<origem2> <destino> [
<entidade virtual> |
                  -bal <ev_1> <ev_2> ... ] <round-robin | randomico>
<persist>
                  <nenhum | ping | HTTP <URL>>
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
fwnat - Configura regras de conversao de enderecos (NAT)
Uso: fwnat [ajuda | mostra | ativa | desativa]
     fwnat [habilita | desabilita | remove] <pos>
     fwnat inclui <pos> 1-1 <origem> <destino> [ <entidade virtual> |
                  -bal <ev_1> <ev_2> ... ]
     fwnat inclui <pos> n-1 <origem> <destino> [ <entidade virtual> |
                  -bal <ev_1> <ev_2> ... ]
     fwnat inclui <pos> servicos <origem> <destino> [ <entidade
virtual> |
                  -bal <ev_1> <ev_2> ... ] <servico1>...<servico2>
     fwnat inclui <pos> sem_conversao <origem> <destino>
     fwnat inclui <pos> 1-n <origem1>...<origem2> <destino> [
<entidade virtual> |
                  -bal <ev_1> <ev_2> ... ] <round-robin | randomico>
<persist>
                  <nenhum | ping | HTTP <URL>>
     ativa         = ativa conversao de enderecos
     desativa      = desativa conversao de enderecos
     mostra        = mostra todas as regras da tabela de conversao
     inclui        = inclui uma nova regra de conversao
     habilita      = habilita uma regra de conversao desabilitada
     desabilita    = desabilita uma regra de conversao existente
     remove        = remove uma regra de conversao existente
     ajuda         = mostra esta mensagem
Para inclui temos:
     pos           = posicao onde incluir a nova regra na tabela
                     (Pode ser um inteiro positivo ou a palavra FIM
para
                      incluir no final da tabela)
     1-1           = realiza conversao de servidores. Neste caso a
origem deve
                     ser obrigatoriamente uma entidade do tipo maquina
     n-1           = realiza conversao de clientes
     servicos      = realiza conversao apenas para os servicos
citados. Neste
                     caso a origem deve ser obrigatoriamente uma
entidade do
                     tipo maquina
     portas        = realiza conversao apenas para o servico citado.
Neste
                     caso a origem deve ser obrigatoriamente uma
entidade do
                     tipo maquina. Alem disso, o servico visivel
externamente
                     sera' o <servico virtual>
     sem_conversao = nao realiza conversao entre a origem e o destino
     1-n           = realiza balanceamento de carga, ou seja,
possibilita que
                     as varias maquinas origem sejam acessadas pelo
endereco
                     IP configurado na entidade virtual, como se
fossem uma so
                     maquina
     servico1 ...  = lista de nomes dos servicos para a nova regra.
Sao aceitos
                     apenas servicos dos protocolos TCP ou UDP
Para habilita / desabilita / remove temos:
     pos           = numero da regra a ser habilitada, desabilitada ou
```

```
removida
                    da tabela
Para conversao 1-n temos:
     round-robin   = Utiliza algoritmo round-robin para o
balanceamento das
                    conexoes
     randomico     = Utiliza algoritmo randomico para o balanceamento
das
                    conexoes
     persist       = Tempo de persistencia (mins) de servidor destino
para
                    conexoes originadas do mesmo cliente
     nenhum        = Nao monitora as maquinas origem, isto e',
considera que
                    elas estao sempre ativas
     ping          = Monitora as maquinas origem atraves de pings
     HTTP          = Monitora as maquinas origem atraves de conexoes
HTTP
     URL           = Especifica qual a URL deve utilizada para
monitorar as
                    maquinas, no caso de se utilizar monitoramento
HTTP
```

Exemplo 1 : (Mostrando a configuração)

```
#/etc/firewall/fwnat mostra

Parametros Globais:
-------------------

Conversao de enderecos: Ativada

Regras de Conversao:
--------------------

Regra 01
--------
Tipo            : sem_conversao
Origem          : Rede Interna
Destino         : Rede Interna

Regra 02
--------
Tipo            : servicos
Origem          : Server
Destino         : Internet
Entidade virtual: Firewall - interface externa
Servicos        : MYSQL                    POP3
                  SMTP

Regra 03
--------
Tipo            : 1-1

Origem          : Web Server_001
Destino         : Internet
Entidade virtual: External Web server

Regra 04
--------
Tipo            : 1-n
```

```
Origem          : server1
server2
                  server3
Destino         : Internet
Entidade virtual: Virtual Server
Balanceamento   : randomico    Monitoramento: http
URL             : www.aker.com.br

Regra 05
--------
Tipo            : n-1
Origem          : Rede Interna
Destino         : Internet
Entidade virtual: Firewall - interface externa
```

Exemplo 2 : (Incluindo uma regra de conversão 1-1 no final da tabela. mapeando o servidor *SMTP Server*, com endereço reservado para o *External Server*, com endereço válido para todas as máquinas da Internet)

```
#/etc/firewall/fwnat inclui fim 1-1 "SMTP Server" Internet "External
Server"
Regra incluida na posicao 6
```

Exemplo 3 : (Incluindo uma regra de conversão de serviços no início da tabela)

```
#/etc/firewall/fwnat inclui 1 Servicos "Server 2" Internet "External
Server 2" Telnet FTP
Regra incluida na posicao 1
```

Exemplo 4 : (Removendo a regra 3)

```
#/etc/firewall/fwnat remove 3
Regra 5 removida
```

Exemplo 5 : (Incluindo uma regra de conversão 1-N, balanceamento, mapeando os servidores *srv01* e *srv02* em uma máquina externa chamada de *srv_externo*, para todas as máquinas da Internet, e monitorando via ping)

```
#/etc/firewall/fwnat inclui 4 1-N srv01 srv02 Internet srv_externo
round-robin ping
Regra incluida na posicao 4
```

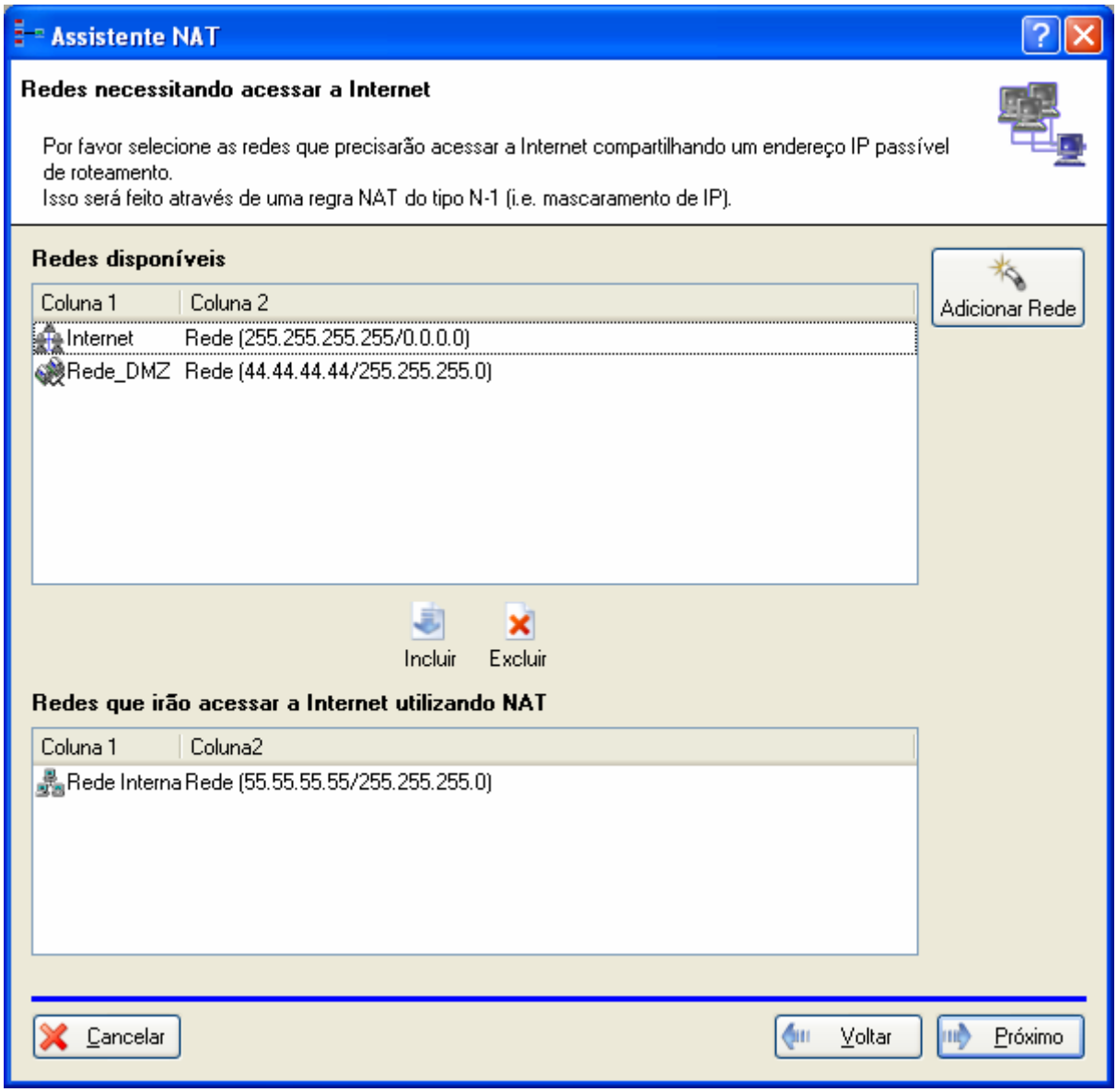
7-4 Utilizando o Assistente de Configuração NAT

O assistente de configuração NAT pode ser acionado tanto pela barra de ferramentas como pelo menu. As janelas abaixo irão solicitar diversas informações de modo a ser configurada a conversão.

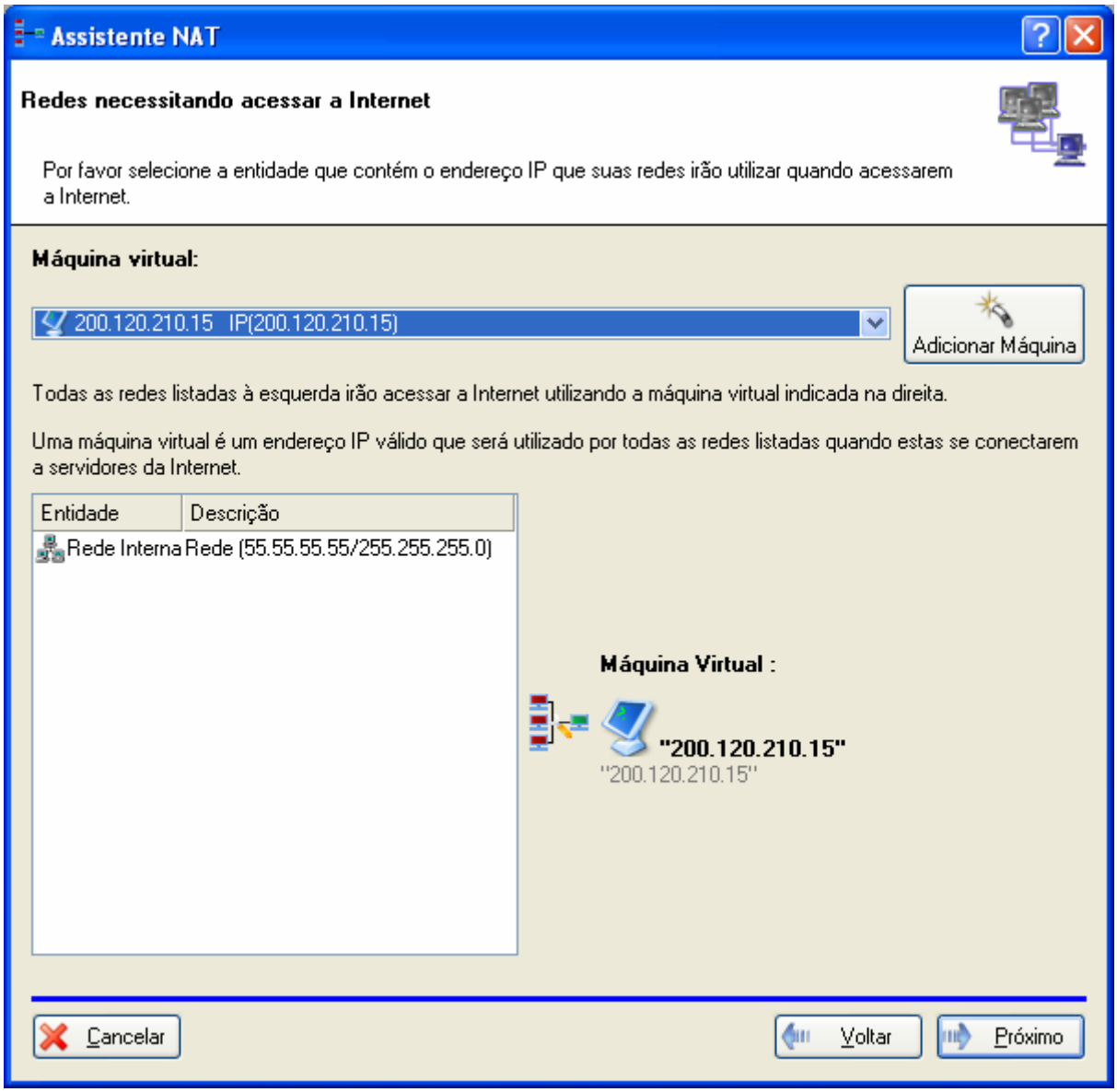
1 - A janela inicial informa sobre o que é o NAT. Clique no botão Próximo para continuar com a configuração.

Assistente NAT
Assistente de Configuração NAT
Bem-vindo ao Assistente de Configuração NAT
A Conversão de endereços de Rede (NAT) é uma tecnologia que muda os endereços IP presentes em pacotes IP quando eles são processados pelo firewall. Alterando estes endereços de acordo com regras pré-definidas, muitas funcionalidades podem ser adicionadas ao seu firewall. As principais são:
• Possibilidade de que muitas máquinas com endereços IP privados possam acessar a Internet compartilhando um único endereço passível de roteamento.
• Possibilidade de que servidores internos com endereços IP privados possam ser acessíveis pela Inernet.
Este assistente vai ajudá-lo a configurar ambas estas funcionalidades. Depois de finalizado, um conjunto de novas regras será criado, as quais poderão ser posteriomente refinadas com o objetivo de ativar outras funcionalidades avançadas encontradas no NAT do Aker Firewall, como balanceamento de link e de carga do servidor.
Aviso: Todas as regras existentes serão desabilitadas se você completar este assistente.
Cancelar
Voltar
Próximo

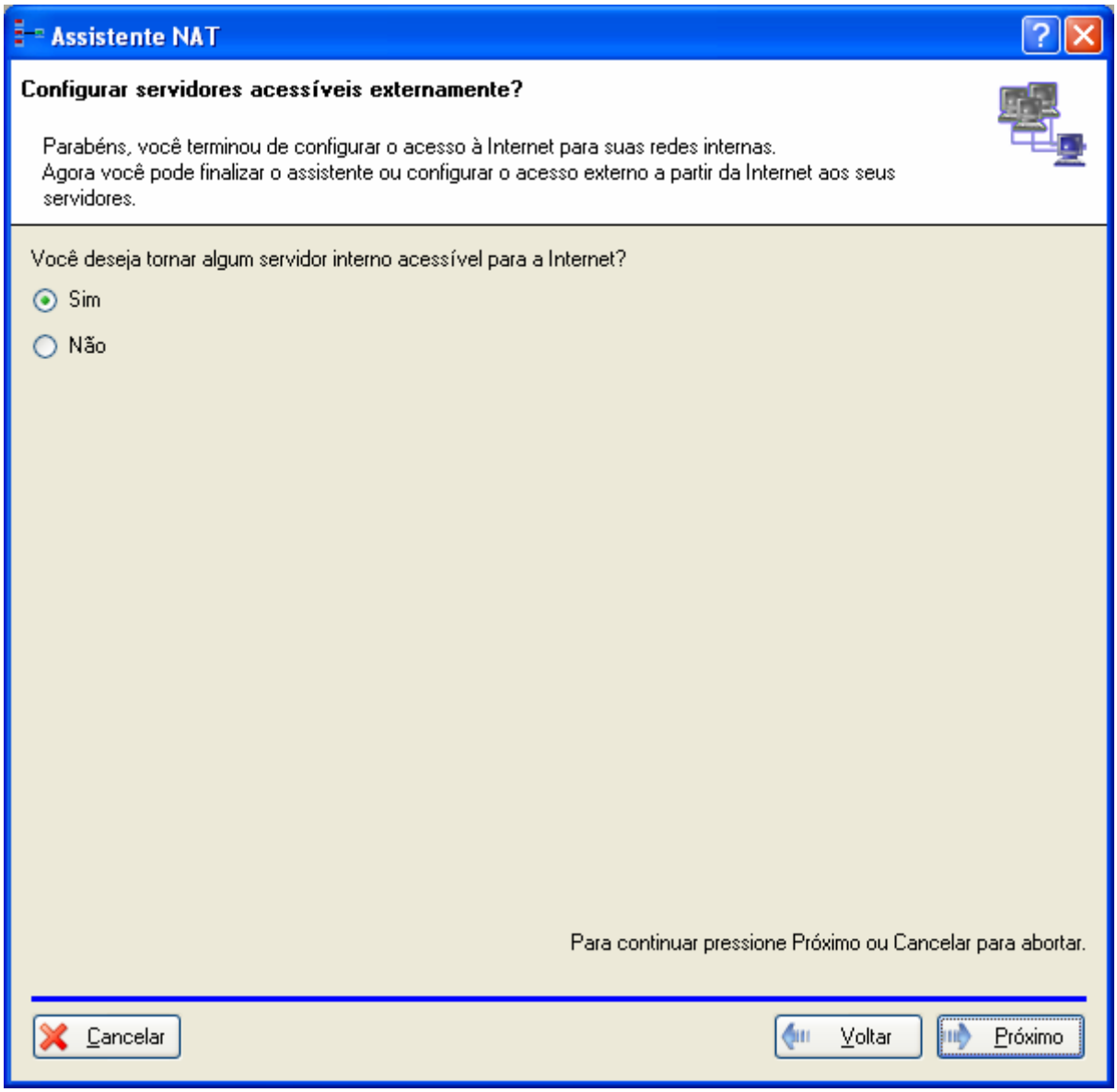
2 - Informe as redes que necessitarão acessar a Internet



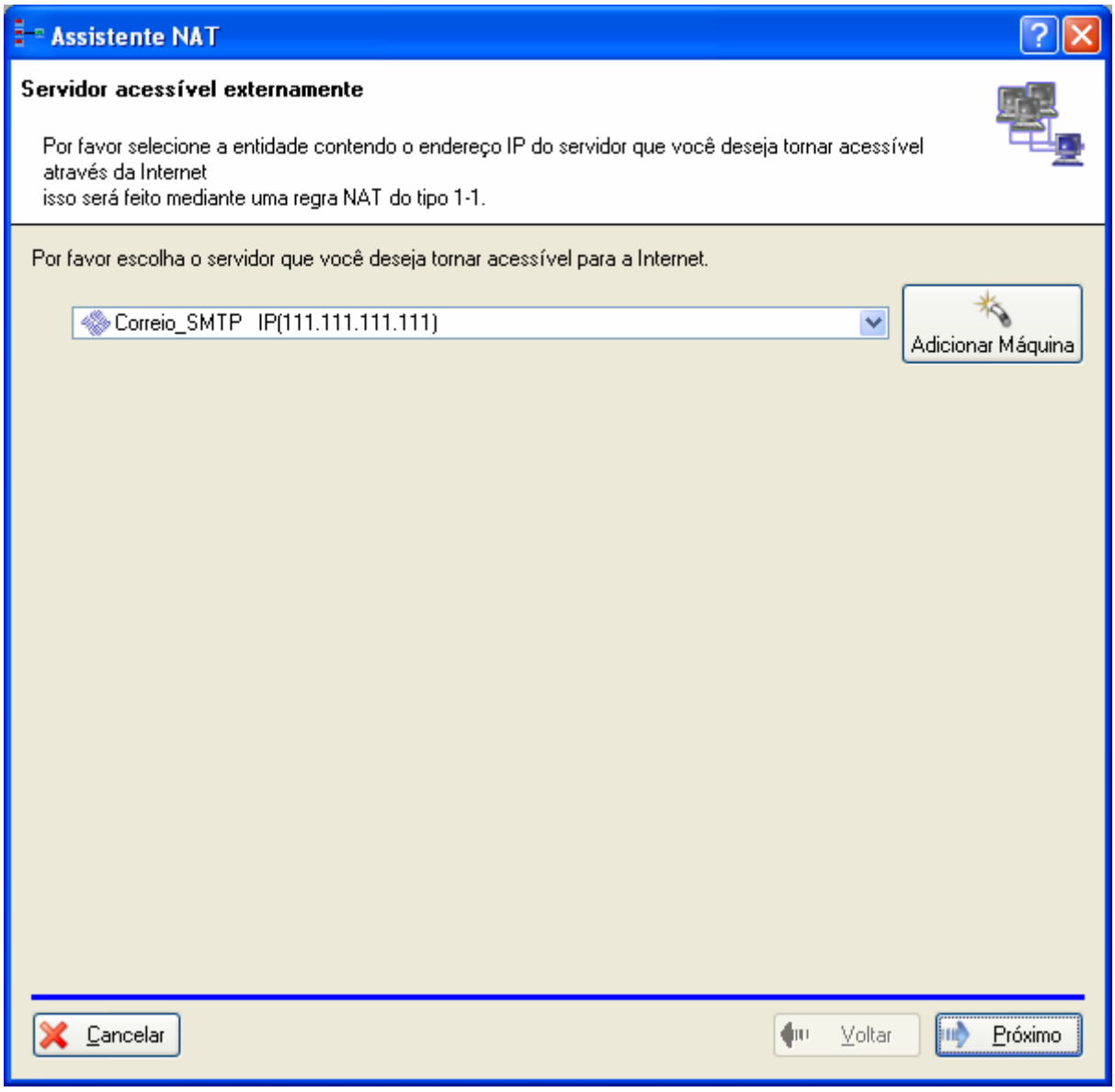
3 - Escolha o IP da Máquina virtual para realizar a conversão N-1


Assistente NAT
Redes necessitando acessar a Internet
Por favor selecione a entidade que contém o endereço IP que suas redes irão utilizar quando acessarem a Internet.
Máquina virtual:
200.120.210.15 IP(200.120.210.15)
Adicionar Máquina
Todas as redes listadas à esquerda irão acessar a Internet utilizando a máquina virtual indicada na direita.
Uma máquina virtual é um endereço IP válido que será utilizado por todas as redes listadas quando estas se conectarem a servidores da Internet.
Entidade
Descrição
Rede Interna
Rede (55.55.55.55/255.255.255.0)
Máquina Virtual :
"200.120.210.15"
"200.120.210.15"
Cancelar
Voltar
Próximo

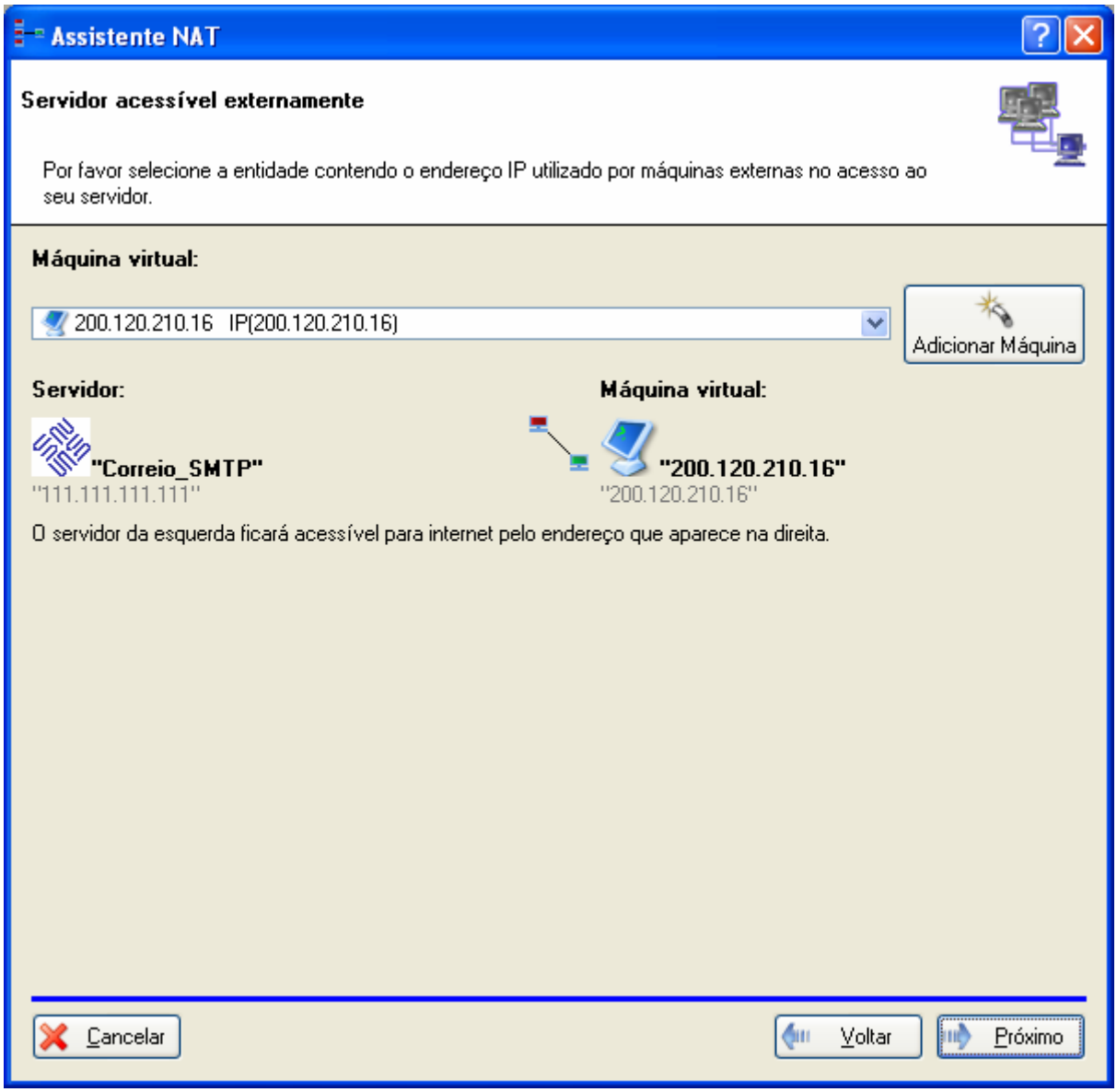
4 - Escolha a opção *Sim* caso queira configurar os servidores que deverão aparecer para Internet.


Assistente NAT
Configurar servidores acessíveis externamente?
Parabéns, você terminou de configurar o acesso à Internet para suas redes internas.
Agora você pode finalizar o assistente ou configurar o acesso externo a partir da Internet aos seus servidores.
Você deseja tornar algum servidor interno acessível para a Internet?
Sim
Não
Para continuar pressione Próximo ou Cancelar para abortar.
Cancelar
Voltar
Próximo

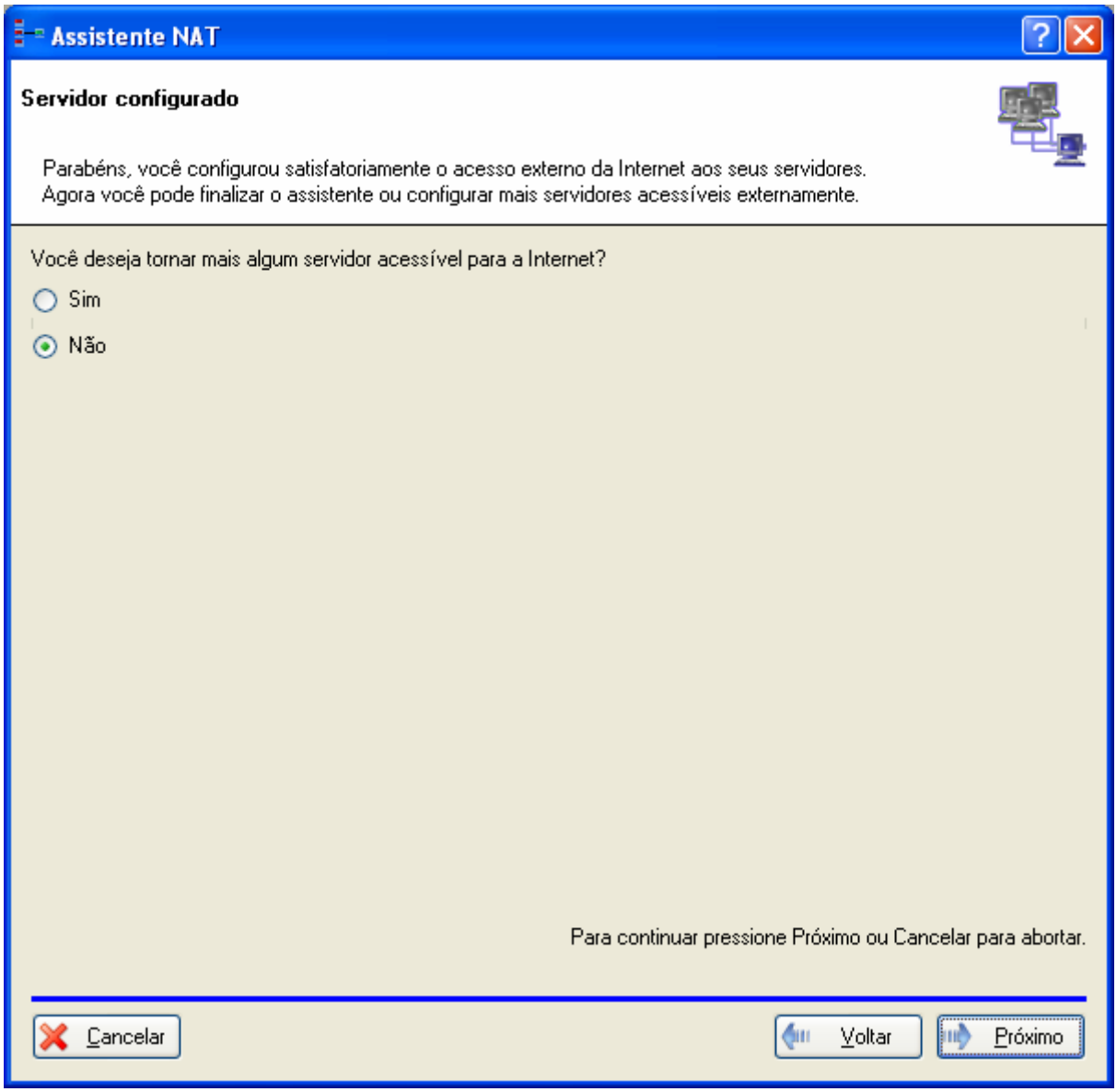
5 - Escolha a entidade para aparecer para a Internet


Assistente NAT
Servidor acessível externamente
Por favor selecione a entidade contendo o endereço IP do servidor que você deseja tornar acessível através da Internet
isso será feito mediante uma regra NAT do tipo 1-1.
Por favor escolha o servidor que você deseja tornar acessível para a Internet.
Correio_SMTP IP(111.111.111.111)
Adicionar Máquina
Cancelar
Voltar
Próximo

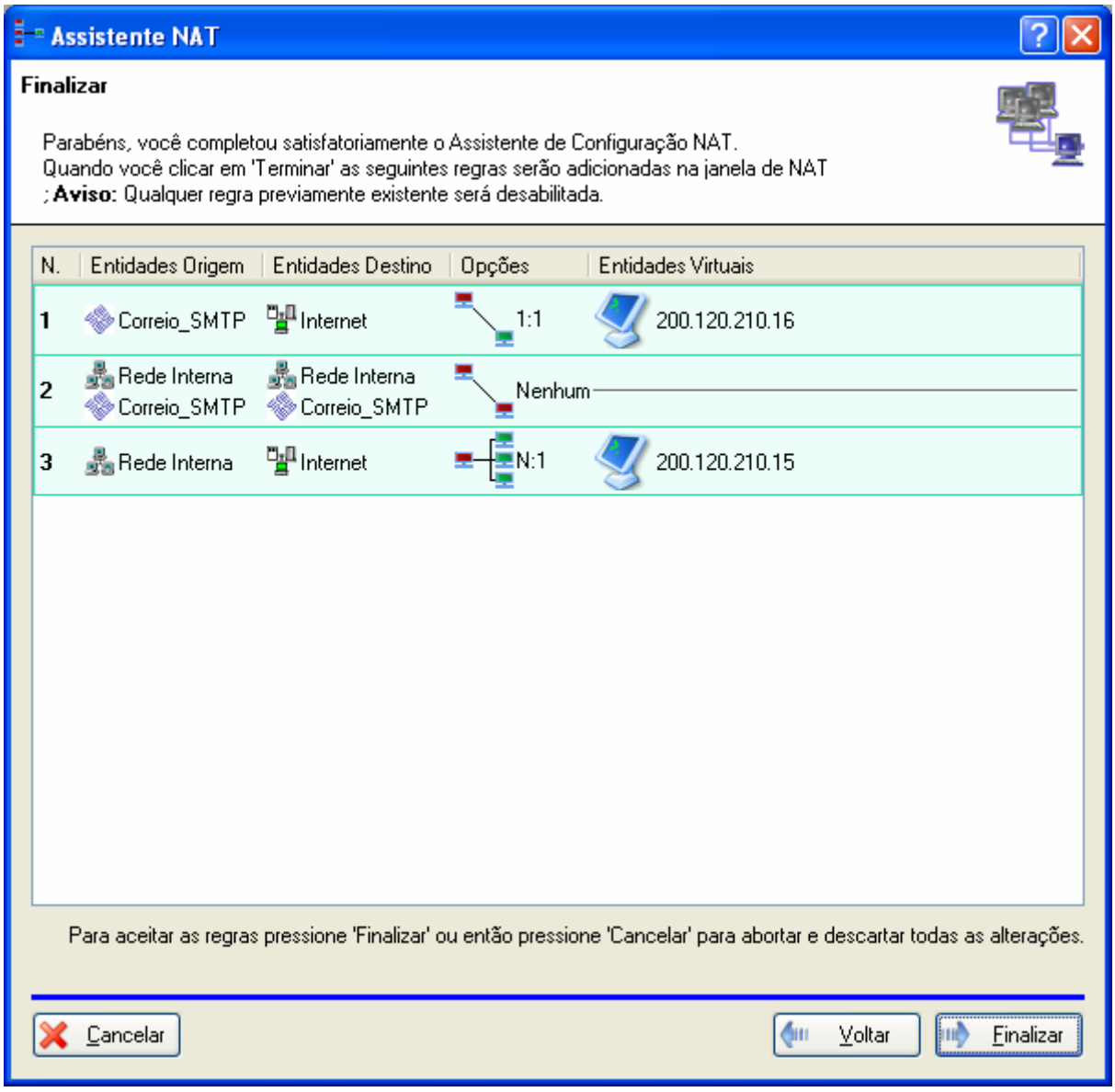
6 - Escolha o IP da Máquina virtual o qual o servidor será mostrado para Internet.



7 - Este tela irá permitir que mais servidores sejam configurados.


Assistente NAT
Servidor configurado
Parabéns, você configurou satisfatoriamente o acesso externo da Internet aos seus servidores.
Agora você pode finalizar o assistente ou configurar mais servidores acessíveis externamente.
Você deseja tornar mais algum servidor acessível para a Internet?
Sim
Não
Para continuar pressione Próximo ou Cancelar para abortar.
Cancelar
Voltar
Próximo

8 - Tela de finalização do Assistente e regras que foram criadas pelo mesmo


Assistente NAT
Finalizar
Parabéns, você completou satisfatoriamente o Assistente de Configuração NAT.
Quando você clicar em 'Terminar' as seguintes regras serão adicionadas na janela de NAT
; Aviso: Qualquer regra previamente existente será desabilitada.
N.
Entidades Origem
Entidades Destino
Opções
Entidades Virtuais
1
Correio_SMTP
Internet
1:1
200.120.210.16
2
Rede Interna
Correio_SMTP
Rede Interna
Correio_SMTP
Nenhum
3
Rede Interna
Internet
N:1
200.120.210.15
Para aceitar as regras pressione 'Finalizar' ou então pressione 'Cancelar' para abortar e descartar todas as alterações.
Cancelar
Voltar
Finalizar

8-0 Criando Canais de Criptografia

Mostraremos aqui como configurar as regras que propiciarão a criação de canais seguros de comunicação na Internet. Estes canais seguros são usados para interligar instituições pela Internet de forma com que os dados fluam entre elas sem o risco de serem lidos ou alterados por estranhos.

8-1 Planejando a instalação.

O que é e para que serve um canal seguro de dados ?

A Internet é uma rede mundial composta de milhares de máquinas espalhadas por todo o mundo. Quando duas máquinas quaisquer estão se comunicando, todo o tráfego entre elas passa por diversas outras máquinas (roteadores, switches, etc) desde sua origem até seu destino. Na quase totalidade das vezes, a administração destas máquinas intermediárias é feita por terceiros e nada se pode afirmar quanto a sua honestidade (na maioria das vezes, não é nem possível se saber de antemão por quais máquinas os pacotes passarão até atingir seu destino).

Qualquer uma destas máquinas que estiver no caminho dos pacotes pode visualizar seu conteúdo e/ou alterar qualquer um destes. Isto é um problema sério e sua importância é aumentada ainda mais quando existe a necessidade de se transmitir dados confidenciais e de grande impacto.

Para se resolver este problema, pode-se usar um canal seguro de dados. Um canal seguro de dados pode ser visto como se fosse um túnel. De um lado são colocadas as informações que só poderão ser lidas novamente após saírem do outro lado.

Na prática, o que é feito é dar um tratamento especial aos dados a serem transmitidos de modo que estes não possam ser alterados durante seu caminho (autenticação), nem visualizados (criptografia). A combinação das duas técnicas produz dados invisíveis e imutáveis para qualquer máquina que se encontre no caminho dos pacotes, da origem ao destino.

O que é criptografia ?

Criptografia é a combinação de uma chave com um algoritmo matemático baseado em uma função unidirecional. Este algoritmo é aplicado aos dados, juntamente com a chave, de modo a torná-los indecifráveis para qualquer um que os veja. O modo que isso é feito garante que somente é possível se obter os dados originais caso se possua o algoritmo e a chave usados inicialmente.

Mantendo-se um destes dois componentes secretos (no caso, a chave), faz-se com que a visualização dos dados por terceiros se torne impossível.

O que é autenticação ?

Autenticação é também a combinação de uma chave com um algoritmo matemático baseado em uma função unidirecional. A diferença em relação a criptografia, é que este algoritmo, quando aplicado sobre os dados, não produz dados indecifráveis mas sim uma *assinatura digital* para estes. Essa assinatura é gerada de tal forma que qualquer pessoa que desconheça o algoritmo ou a chave utilizados para gerá-la seja incapaz de calculá-la.

Quando a assinatura digital é gerada, ela passa a ser transmitida para o destino junto com os dados. Caso estes tenham sofrido quaisquer alterações no caminho, o recipiente quando calcular a assinatura digital dos dados recebidos e compará-la com a assinatura recebida, irá perceber que as duas são diferentes e concluir que os dados foram alterados.

A autenticação é uma operação bastante rápida quando comparada com a criptografia, porém ela sozinha não consegue impedir que os dados sejam lidos. Ela deve ser usada apenas nos casos onde se necessita confiabilidade dos dados mas não sigilo. Caso se necessite de ambos, usa-se autenticação em conjunto com a criptografia.

O que é certificação digital ?

Através do processo de autenticação descrito acima, é possível se garantir a origem das mensagens em uma comunicação entre duas partes. Entretanto, para que isso seja possível, é necessário que as entidadades que estão se comunicando já tenham previamente trocado informações através de algum meio fora do tráfego normal dos dados. Esta troca de informações normalmente consiste no algoritmo a ser utilizado para a autenticação e sua chave.

O problema surge quando se torna necessário assegurar a origem das mensagens de uma entidade com a qual nunca existiu comunicação prévia. A única forma de se resolver este problema é delegar a uma terceira entidade o poder de realizar estas autenticações (ou em termos mais técnicos, realizar a certificação da origem de uma mensagem). Esta terceira entidade é chamada de **Entidade Certificadora** e, para que seja possível ela assegurar a origem de uma mensagem, ela já deve ter realizado uma troca de informações com a entidade que está sendo certificada.

O que é um certificado digital ?

Certificado digital é um documento fornecido pela Entidade Certificadora para cada uma das entidades que irá realizar uma comunicação, de forma a garantir sua autenticidade.

Tipos de algoritmos de autenticação e criptografia

Existem inúmeros algoritmos de autenticação e criptografia existentes atualmente. Neste tópico serão mostrados apenas os algoritmos suportados pelo Firewall Aker.

Cabe comentar que um dos parâmetros para se medir a resistência de um algoritmo é o tamanho de suas chaves. Quanto maior o número de bits das chaves, maior o número de

possíveis combinações e, teoricamente, maior é a resistência do algoritmo contra ataques.

Algoritmos de autenticação:

- MD5

MD5 é a abreviatura de *Message Digest 5*. Ele é um algoritmo criado e patenteado pela RSA Data Security, Inc, porém com uso liberado para quaisquer aplicações. Ele é usado para gerar assinaturas digitais de 128 bits para mensagens de qualquer tamanho e é considerado um algoritmo bastante rápido e seguro.

- SHA

SHA é a abreviatura de *Secure Hash*. Ele é um algoritmo que gera assinaturas digitais de 160 bits para mensagens de qualquer tamanho. Ele é considerado mais seguro que o MD5, porém tem uma performance em média 50% inferior (na implementação do Firewall Aker).

A versão implementada pelo Firewall Aker é o SHA-1, uma revisão no algoritmo inicial para corrigir uma pequena falha. Entretanto ele será chamado sempre de SHA, tanto neste manual quanto nas interfaces de administração.

Algoritmos de criptografia simétricos:

Os algoritmos de criptografia simétricos são utilizados para se encriptar fluxos de informações. Eles possuem uma única chave que é utilizada tanto para encriptar quanto para decriptar os dados.

- DES

O algoritmo DES, que é um anagrama para *Data Encription Standard*, foi criado pela IBM na década de 70 e foi adotado pelo governo americano como padrão até recentemente. Ele é um algoritmo bastante rápido em implementações de hardware, porém não tão rápido quando implementado em software. Suas chaves de criptografia possuem tamanho fixo de 56 bits, número considerado pequeno para os padrões atuais. Devido a isso, deve-se dar preferência a outros algoritmos em caso de aplicações críticas.

- Triplo DES ou 3DES

Este algoritmo consiste na aplicação do algoritmo DES três vezes, usando três chaves distintas, sobre os mesmos dados. Isto equivale a se utilizar um algoritmo com chave de 112 bits, o que representa uma segurança extremamente maior do que a oferecida pelo DES. O problema deste algoritmo é que ele é duas vezes mais lento que o DES (na implementação utilizada no Firewall Aker).

- AES

O algoritmo AES foi escolhido dentre muitos concorrentes pelo NIST para substituir o já inseguro e ineficiente DES. AES é um anagrama para *Advanced Encryption Standard*. O algoritmo escolhido em concurso foi o Rijndael, e ele utiliza 256 bits de chave, sendo ao mesmo tempo muito mais seguro e rápido que o DES ou mesmo o 3DES.

O Firewall Aker trabalha com o AES utilizando chaves de 256 bits, o que garante um nível altíssimo de segurança. Ele é a escolha recomendada.

- Blowfish

O algoritmo Blowfish foi criado como uma possível substituição ao DES. Ele é um algoritmo extremamente rápido (quando comparado com outros algoritmos de criptografia), bastante seguro e pode trabalhar com vários tamanhos de chaves, de 40 a 438 bits.
O Firewall Aker trabalha com o Blowfish utilizando chaves de 128 ou 256 bits, o que garante um nível altíssimo de segurança.
Algoritmos de criptografia assimétricos:
Os algoritmos de criptografia assimétricos possuem um par de chaves associadas, uma para encriptar e outra para decriptar os dados. Eles são bastante lentos se comparados aos algoritmos simétricos e, devido a isso, normalmente são utilizados apenas para realizar assinaturas digitais e no estabelecimento de chaves de sessão que serão usadas em algoritmos simétricos.

- RSA

O RSA é um algoritmo baseado em aritmética modular capaz de trabalhar com chaves de qualquer tamanho, porém valores inferiores a 512 bits são considerados muito frágeis. Ele pode ser utilizado para encriptar e decriptar dados, porém, devido a sua grande lentidão se comparado aos algoritmos simétricos, seu principal uso é em assinaturas digitais e no estabelecimento de chaves de sessão.

- Diffie-Hellman

O algoritmo Diffie-Hellman na verdade não pode ser encarado como algoritmo de criptografia, uma vez que não serve para encriptar dados ou realizar assinaturas digitais. Sua única função é possibilitar a troca de chaves de sessão, feita de forma a impedir que escutas passivas no meio de comunicação consigam obtê-las. Ele também é baseado em aritmética modular e pode trabalhar com chaves de qualquer tamanho, porém chaves menores que 512 são consideradas muito frágeis.

Algoritmos de trocas de chaves

Um problema básico que ocorre quando se configura um canal seguro é como configurar as chaves de autenticação e criptografia e como realizar trocas periódicas destas chaves.
É importante realizar trocas periódicas de chaves para diminuir a possibilidade de quebra das mesmas por um atacante e para diminuir os danos causados caso ele consiga decifrar uma das chaves: Suponha que um atacante consiga em seis meses quebrar as chaves usadas por um algoritmo de criptografia (este tempo é totalmente hipotético, não

tendo nenhuma relação com situações reais). Se uma empresa usar as mesmas chaves durante, digamos, 1 ano, então um atacante conseguirá decifrar todo o tráfego nos últimos 6 meses desta empresa. Em contrapartida, se as chaves forem trocadas diariamente, este mesmo atacante, após 6 meses, conseguirá decifrar o tráfego do primeiro dia e terá mais 6 meses de trabalho para decifrar o tráfego do segundo dia e assim por diante.
O Firewall Aker possui quatro métodos para trocas de chaves: IPSEC-IKE, AKER-CDP, SKIP e manual:

- Troca de chaves via IPSEC-IKE

  Esta opção estará disponível apenas quando se utilizar o conjunto completo de protocolos IPSEC.

  O IPSEC (*IP Security*) é um conjunto de protocolos padronizados (RFC 2401-RFC 2412) desenvolvidos pela IETF. O IPSec oferece transferência segura de informações através de rede IP pública ou privada. Uma conexão via IPSec envolve sempre 3 etapas:

  1. Negociação do nível de segurança.
  2. Autenticação e Integridade.
  3. Confidencialidade.

  Para implementar essas 3 etapas o IPSec utiliza-se de 3 mecanismos:

  AH - Autentication Header
  ESP - Encapsulation Security Payload
  IKE - Internet Key Exchange Protocol

  Recomenda-se fortemente o uso desta opção na hora de se configurar os canais seguros.

- Troca de chaves via Aker-CDP

  O Aker-CDP é um protocolo designado pela Aker Security Solutions que possibilita a configuração totalmente automática de todos os parâmetros de um canal seguro. Ele utiliza o protocolo SKIP como base (o que significa que ele oferece todas as facilidades de trocas de chaves apresentadas anteriormente), porém possui a grande vantagem de não necessitar de uma configuração manual dos segredos compartilhados, tudo é feito automaticamente.

  Para assegurar o máximo de segurança, toda a troca de chaves é feita através de certificados digitais assinados pela própria Aker ou por outras entidades certificadoras autorizadas. Nestes certificados são utilizados os protocolos Diffie-Hellman e RSA, ambos com 1024 bits.

  Os algoritmos a serem utilizados na criptografia e autenticação podem ser especificados, da mesma forma que no protocolo SKIP, ou deixados em modo automático, o que fará que os dois firewalls comunicantes negociem o algoritmo mais seguro suportado por ambos.

- Troca de chaves via SKIP

  SKIP é um anagrama para *Simple Key Management for IP*. Ele é basicamente um algoritmo que permite que as trocas de chaves sejam realizadas de forma automática e com uma freqüência extremamente elevada, tornando inviável a quebra destas chaves. O funcionamento do SKIP é complexo e não entraremos em maiores detalhes aqui. Nossa abordagem se limitará a descrever seu funcionamento.
  Basicamente o SKIP trabalha com três níveis diferentes de chaves:

- Um segredo compartilhado pelas duas entidades que desejam se comunicar (configurado manualmente, no caso do Firewall Aker).
- Uma chave mestre, recalculada de hora em hora, baseada no segredo compartilhado
- Uma chave randômica, que pode ser recalculada quando se desejar.

  Genericamente falando, para efetuar a comunicação, o algoritmo gera um chave aleatória e a utiliza para encriptar e autenticar os dados a serem enviados. A seguir ele encripta esta chave com a chave mestre e envia isto junto com os dados encriptados. Ao receber o pacote, o outro lado decripta a chave, com o auxílio da chave mestra, e a utiliza para decriptar o restante do pacote.

  Os algoritmos utilizados para autenticar o pacote, encriptá-lo e encriptar a chave são definidos pelo remetente e informados como parte do protocolo. Desta forma, não é necessário se configurar estes parâmetros no recipiente.

  A principal vantagem do SKIP é a possibilidade de se utilizar o mesmo segredo compartilhado por anos, sem a menor possibilidade de quebra das chaves por qualquer atacante (uma vez que a troca de chaves é efetuada em intervalos de poucos segundos a no máximo uma hora, dependendo do tráfego entre as redes comunicantes).

- Troca de chaves manual

  Neste caso, toda a configuração de chaves é feita manualmente. Isto implica que todas as vezes que uma chave for trocada, ambos os Firewall participantes de um canal seguro terão que ser reconfigurados simultaneamente.

Tipos de canais seguros

O Firewall Aker possibilita a criação de dois tipos de canais seguros distintos, chamados de Firewall-Firewall e Cliente-Firewall. Cada um destes tipos de canais possuem objetivos e limitações diferentes e normalmente são combinados para se atingir o máximo de segurança e flexibilidade.

- Canais seguros Firewall-Firewall

Este tipo de canal seguro é o mais comum e é suportado pelo Firewall Aker desde sua versão 1.31. Ele consiste na utilização de criptografia e autenticação entre dois

firewalls, interligados através da Internet ou de outro meio qualquer. Os pontos de entrada e saída do canal são os dois firewalls, o que significa que toda a criptografia é feita transparentemente por eles e nenhum software adicional necessita ser instalado em nenhuma máquina cliente.

A única limitação desta solução é que ela exige a presença de dois firewalls, um na entrada de cada rede, para que o canal seguro possa ser criado.

- Canais seguros Cliente-Firewall

Estes canais são suportados pelo Firewall Aker a partir da versão 3.10. Eles permitem com que uma máquina cliente (Windows 95™, Windows 98™, Windows NT™ ou Windows 2000™) estabeleça um canal seguro diretamente com um Firewall Aker. Para tanto, é necessária a instalação de um programa, chamado de cliente de criptografia Aker, em cada uma destas máquinas.

A principal vantagem desta tecnologia é possibilitar com que clientes acessem uma rede coorporativa através de linhas discadas com total segurança e transparência (transparência na medida em que as aplicações que estejam rodando na máquina com o cliente de criptografia instalado desconhecem sua existência e continuam funcionando normalmente).

Apesar de bastante útil, esta tecnologia possui algumas desvantagens e limitações:

- É necessário a instalação de um software, cliente de criptografia Aker, em todas as máquinas clientes;
- O cliente de criptografia não está disponível para todas as plataformas;
- Se o cliente de criptografia está atrás de um firewall (acessando a rede protegida por um outro firewall, com o qual o canal seguro será estabelecido), a configuração deste último deve ser alterada para possibilitar a passagem do tráfego do canal seguro. Neste caso, o firewall diretamente na frente do cliente não terá como controlar seu tráfego seletivamente, uma vez que este está encriptado. Isso poderá acarretar problemas de funcionamento de alguns serviços.

Definindo um canal seguro firewall-firewall

Para definirmos um canal seguro firewall-firewall teremos que primeiro escolher dois grupos de máquinas que irão trocar informações entre si de forma segura. Estes grupos de máquinas terão seus pacotes autenticados e, caso desejado, criptografados. É necessário que exista um firewall nas duas extremidades do canal. Estes firewalls serão responsáveis por autenticar/verificar e criptografar/decriptar os dados a serem transmitidos e recebidos, respectivamente.

Para se definir os grupos de máquinas, será utilizado o conceito de entidades, mostrado no capítulo intitulado Cadastrando Entidades. Pode-se utilizar entidades do tipo máquina, rede ou conjunto nesta definição.

Caso não se esteja utilizando o protocolo Aker-CDP, além das entidades, é necessário também se definir o algoritmo que será usado na autenticação e, se for o caso, na

criptografia.Também será necessário se definir as chaves de autenticação e criptografia a serem utilizadas no canal.

O Firewall Aker suporta a existência de diversos canais seguros simultâneos, entre pontos distintos. A união destes diversos canais produz uma lista, onde cada entrada define completamente os parâmetros de um canal seguro. Cada uma destas entradas recebe o nome de *Associação de Segurança ou SA*.

O planejamento destes canais seguros deverá ser feito com bastante cuidado. A criptografia é um recurso dispendioso que demanda uma capacidade de processamento muito alta. Desta forma, criptografar pacotes para os quais não exista uma necessidade real de segurança será um desperdício de recursos. Além disso, deve-se atentar que diferentes algoritmos de criptografia exigem quantidades de processamento diferentes e, por conseguinte, produzem um nível de segurança mais elevado. Dependendo do nível de segurança desejado, pode-se optar por um ou outro algoritmo (a descrição da cada algoritmo suportado pelo Firewall Aker se encontra no tópico anterior).

Uma última observação sobre canais de criptografia firewall-firewall é que estes são unidirecionais, ou seja, caso se deseje configurar uma comunicação segura entre duas redes, A e B, deve-se configurar dois canais diferentes: um canal com origem na rede A e destino na rede B e outro com origem na rede B e destino na rede A. Os pacotes que forem enviados de A para B seguirão a configuração do primeiro canal e os pacotes de B para A seguirão a configuração do segundo. Isto será ilustrado com mais clareza nos exemplos abaixo:

Exemplos do uso de canais seguros firewall-firewall

Exemplo básico de configuração de um canal seguro firewall-firewall

Neste exemplo será mostrado como definir um canal seguro de comunicação entre duas redes, através da Internet, usando dois Firewalls Aker. O canal será criado de forma com que toda a comunicação entre estas duas redes seja segura. Como algoritmo de autenticação foi escolhido o MD5 e como algoritmo de criptografia, o DES.

É obrigatório o uso de um algoritmo de autenticação para todos os fluxos, ou seja, não é permitida a criação de fluxos com criptografia apenas. Isto é necessário já que sem a autenticação os algoritmos de criptografia são passíveis de ataques de recortar e colar (*cut and paste).*

- **Configuração do Firewall Aker da rede 1**

Entidades:

REDE1 - Endereço IP: **A1.B1.C1.0** - Máscara **255.255.255.0**
REDE2 - Endereço IP: **A2.B2.C2.0** - Máscara **255.255.255.0**

Regra de criptografia 1:

Sentido do canal: **envia**
Entidades origem: **REDE1**
Entidades destino: **REDE2**
Algoritmo de criptografia: **DES**
Algoritmo de autenticação: **MD5**
Chave de autenticação: **X1**
Chave de criptografia: **X2**

Regra de criptografia 2:

Sentido do canal: **recebe**
Entidades origem: **REDE2**
Entidades destino: **REDE1**
Algoritmo de criptografia: **DES**
Algoritmo de autenticação: **MD5**
Chave de autenticação: **X3**
Chave de criptografia: **X4**

- **Configuração do Firewall Aker da rede 2**

Entidades:

REDE1 - Endereço IP: **A1.B1.C1.0 -** Máscara **255.255.255.0**
REDE2 - Endereço IP: **A2.B2.C2.0 -** Máscara **255.255.255.0**

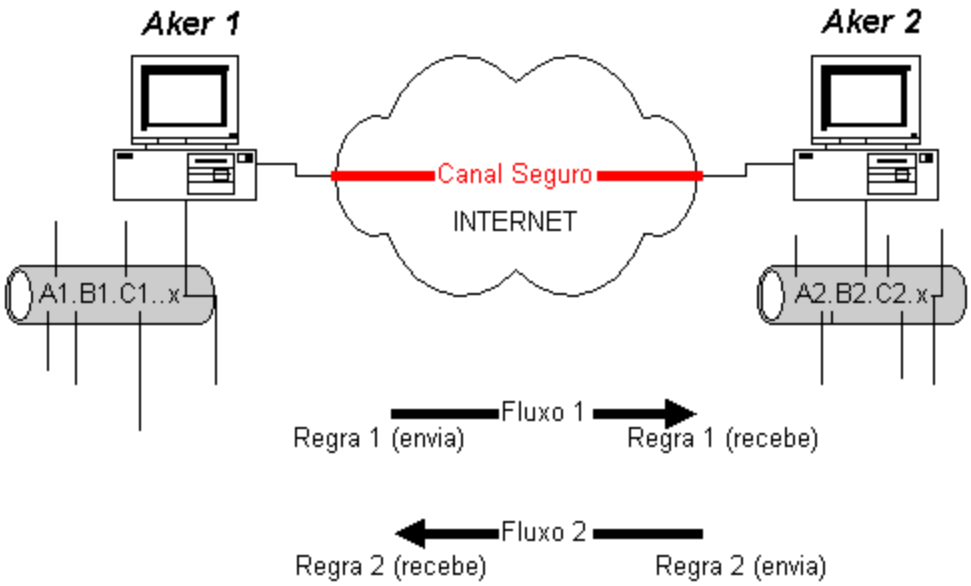
Regra de criptografia 1:

Sentido do canal: **recebe**
Entidades origem: **REDE1**
Entidades destino: **REDE2**
Algoritmo de criptografia: **DES**
Algoritmo de autenticação: **MD5**
Chave de autenticação: **X1**
Chave de criptografia: **X2**

Regra de criptografia 2:

Sentido do canal: **envia**
Entidades origem: **REDE2**
Entidades destino: **REDE1**
Algoritmo de criptografia: **DES**
Algoritmo de autenticação: **MD5**
Chave de autenticação: **X3**
Chave de criptografia: **X4**

Note que a regra 1 do *Firewall Aker 1* é exatamente igual à regra 1 do *Firewall Aker 2*, exceto no campo relativo ao *sentido*. O mesmo ocorre com as regras 2.



Exemplo de configuração de um canal seguro firewall-firewall para uma sub-rede

Neste exemplo o nosso canal seguro será definido apenas para um grupo de máquinas dentro de cada uma das duas redes. Além disso, definiremos algoritmos diferentes para os fluxos entre estes grupos.

Na prática, configurar algoritmos diferentes para os dois sentidos de um canal seguro pode ser interessante quando as informações de um determinado sentido tiverem um valor maior do que as do sentido oposto do fluxo. Neste caso, utiliza-se um algoritmo mais seguro no sentido mais crítico.
Neste exemplo, vamos supor que as redes 1 e 2 possuam dois endereços classe B: A1.B1.0.0 e A2.B2.0.0, respectivamente.

- **Configuração do Firewall Aker da rede 1**

Entidades:

SUB_REDE1 - Endereço IP: **A1.B1.2.0** - Máscara **255.255.255.0**
SUB_REDE2 - Endereço IP: **A2.B2.5.0** - Máscara **255.255.255.0**

Regra de criptografia 1:

Sentido do canal: **envia**
Entidades origem: **SUB_REDE1**
Entidades destino: **SUB_REDE2**
Algoritmo de criptografia: **DES**
Algoritmo de autenticação: **MD5**
Chave de autenticação: **X1**
Chave de criptografia: **X2**

Regra de criptografia 2:

Sentido do canal: **recebe**
Entidades origem: **SUB_REDE2**

Entidades destino: **SUB_REDE1**
Algoritmo de criptografia: **3DES**
Algoritmo de autenticação: **SHA**
Chave de autenticação: **X3**
Chave de criptografia: **X4**

- **Configuração do Firewall Aker da rede 2**

Entidades:

SUB_REDE1 - Endereço IP: **A1.B1.2.0** - Máscara **255.255.255.0**
SUB_REDE2 - Endereço IP: **A2.B2.5.0** - Máscara **255.255.255.0**

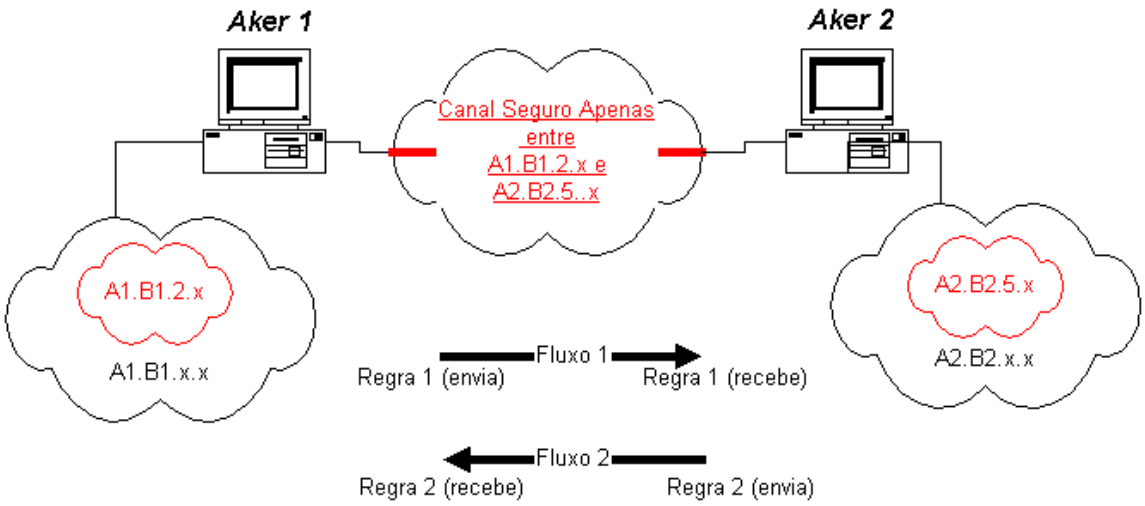
Regra de criptografia 1:

Sentido do canal: **envia**
Entidades origem: **SUB_REDE2**
Entidades destino: **SUB_REDE1**
Algoritmo de criptografia: **3DES**
Algoritmo de autenticação:**SHA**
Chave de autenticação: **X3**
Chave de criptografia: **X4**

Regra de criptografia 2:

Sentido do canal: **recebe**
Entidades origem: **SUB_REDE1**
Entidades destino: **SUB_REDE2**
Algoritmo de criptografia: **DES**
Algoritmo de autenticação: **MD5**
Chave de autenticação: **X1**
Chave de criptografia: **X2**

Note que neste caso as regras aparecem colocadas em uma ordem diferente nos dois firewalls: a regra 1 no Firewall 1 é igual a regra 2 do Firewall 2 (com os sentidos invertidos) e a regra 2 no Firewall 1 é igual a regra 1 no Firewall 2 (novamente com os sentidos trocados). Neste exemplo, a ordem das regras não faz diferença (observe entretanto que em alguns casos isto pode não ser verdade).



8-2 Carregando certificados Aker-CDP

Existem quatro tipos de certificados de criptografia no Firewall Aker. Cada um deles tem objetivos e funções diferentes dentro do protocolo Aker-CDP. São eles:

- Certificado local

Este é o certificado de negociação do firewall que está se administrando. Ele é gerado pela Aker Security Solutions ou por alguma outra entidade certificadora autorizada. Somente pode existir um certificado local e, caso um novo seja carregado, o antigo será automaticamente substituído.

Este certificado será enviado automaticamente para os outros firewalls ou clientes de criptografia quando estes desejarem estabelecer um canal seguro.

- Certificados de negociação

Estes são os certificados locais dos outros firewalls com os quais o firewall que se está administrando recebeu ao negociar canais seguros através do protocolo Aker-CDP.

- Certificados de entidades certificadoras

Estes são os certificados com as informações das entidades certificadoras autorizadas a emitir certificados de negociação e revogação. Para que um destes certificados seja aceito pelo firewall, ele deve obrigatoriamente vir assinado por uma entidade certificadora conhecida pelo firewall.

- Certificados de revogação

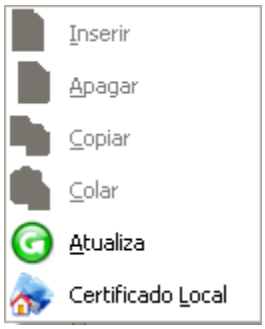
Certificados de revogação são gerados quando ocorre um comprometimento do certificado de negociação de algum firewall. Eles indicam para o firewall que os possui quais certificados não devem mais ser aceitos.
Todos estes certificados podem ser visualizados através da janela de certificados. Para acessá-la, basta:

- Clicar no menu *Criptografia* da janela principal
- Certificados Aker CDP

A janela de certificados

Na janela de certificados são mostrados todos os certificados relacionados ao estabelecimento de canais seguros Aker-CDP.

- O botão **OK** fechará a janela de certificados.
- A lista no lado esquerdo da janela permite a visualização dos diferentes tipos de certificados.
- Ao se clicar sobre um determinado certificado, seus campos principais serão mostrados na lista à direita da janela.
- Ao clicar-se com o botão direito do mouse em cima de um dos campos da janela Certificados, a seguinte janela irá aparecer:



Os campos de cada certificado, mostrados à direita, são apenas informativos. Não é possível se alterar nenhum destes valores.

Para se carregar um novo certificado, deve-se proceder da seguinte forma:

1. Clica-se em um dos botões, clicando com o botão direito do mouse sobre o tipo de certificado que se deseja carregar ou nos botões correspondentes localizados na barra de ferramentas superior. Os tipos de certificados disponíveis são os seguintes : **Certificado Local**, **Autoridade Certificadora** ou **Certificado de Revogação**.
2. Será mostrada uma janela para que se escolha o nome e a localização do arquivo a ser carregado. Após se especificar este nome, deve-se clicar no botão **Abrir**.

Para que se possa utilizar canais seguros firewall-firewall utilizando o protocolo Aker-CDP e ativar o suporte a canais seguros cliente-firewall, é necessário se carregar o certificado de criptografia local, fornecido pela Aker Security Solutions ou seu representante autorizado no momento de compra do Firewall Aker com a opção de criptografia.

8-3 Certificados IPSEC

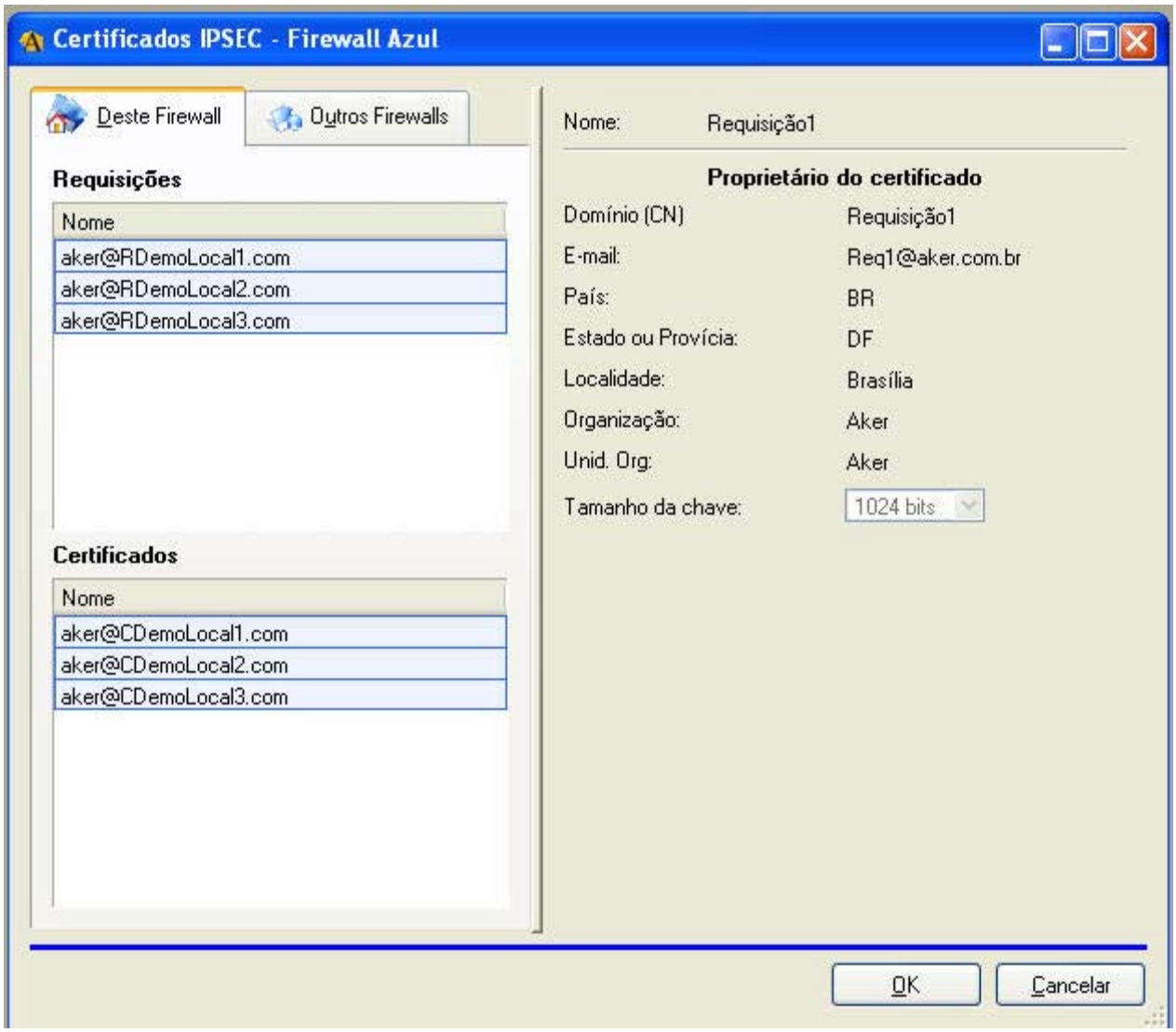
Os certificados IPSEC são certificados padrão X.509 utilizados pelo firewall para identificar-se junto a seus pares quando do estabelecimento dos canais criptográficos firewall-firewall no padrão IPSEC (veja a seção Configurando túneis IPSEC, logo abaixo). Seu uso, entretanto, não é obrigatório, já que é possível se estabelecer canais IPSEC usando segredos compartilhados.

Para que um firewall aceite um certificado apresentado por outro, é preciso que ele possua o certificado da Autoridade Certificadora que o emitiu.

Para ter acesso a janela de manutenção de certificados IPSEC basta:

- Clicar no menu *Criptografia* da janela principal
- Escolher o item *Certificados IPSEC*

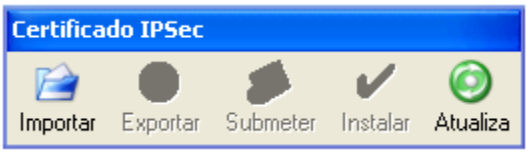
A janela de certificados e requisições IPSEC



A janela de certificados IPSEC contém os certificados e as requisições do Firewall Aker.

Uma requisição é um formulário a ser preenchido com seus dados para que a autoridade certificadora gere um certificado. Um certificado é uma carteira de identidade para autenticar (reconhecer como o próprio) o seu proprietário. O Firewall Aker utilizará estes certificados para se autenticar frente a seus pares quando da negociação de um canal IPSEC. Desta forma cada um dos dois Firewalls envolvidos num canal IPSEC tem que gerar seu próprio certificado.

As operações desta janela se encontram na barra de ferramentas localizada acima da janela de Certificados IPSEC ou clicando-se com o botão direito do mouse sobre o campo que se deseja operar.



- O botão **Inserir** permite se incluir uma nova requisição , podendo ser local ou remota, sendo que as requisições e certificados locais ficam na na janela "*deste firewall*" e certificados e requisições remotas ficam na janela "*outros firewalls*".
- O botão **Apagar** remove da lista o certificado/requisição selecionado.
- O botão **Copiar** copia o certificado/requisição selecionado.
- O botão **Colar** cola da memória o certificado/requisição copiado.
- O botão **Importar** permite que seja carregado um certificado que foi exportado.
- O botão **Exportar** permite que salve o certificado selecionado.
- O botão **Submeter** permite que carregue um certificado exportado ou carregue um certificado de acordo com uma requisição selecionada (somente aparece quando inserindo um novo certificado).
- O botão **Instalar** fará com que a janela seja fechada e atualizada.
- O botão **Atualiza** faz com seja recarregada as informações de certificados.

Para gerar um certificado é necessário que primeiro gere uma requisição no firewall Aker, com esta requisição faça um pedido a uma autoridade certificadora para gerar o certificado e depois importe o certificado para o firewall Aker.

Esta janela é atualizada dinâmicamente, ou seja, não é possível cancelar quando já feito o pedido. Quando incluir-se uma nova requisição local, as requisições e os certificados locais serão apagados. Da mesma forma, ao se importar novo Certificado local com par de chaves (.pfx), serão apagados as requisições e os certificados **locais**.

Desta maneira, a operação deve se dar da seguinte forma (para o certificado local):

1. Criar uma requisição local.
2. Enviar esta requisição a uma Autoridade Certificadora.
3. Esperar até que a Autoridade Certificadora emita o certificado correspondente.
4. Carregar o certificado correspondente à requisição (clicar na requisição e, depois, em *Carregar*)

Se o desejado for criar um certificado para um firewall remoto, o procedimento muda:

1. Criar uma requisição remota.
2. Enviar esta requisição a uma Autoridade Certificadora.
3. Esperar até que a Autoridade Certificadora emita o certificado correspondente.

4. Carregar o certificado correspondente à requisição (clicar na requisição e, depois, em *Carregar*)
5. Exportar o certificado para um arquivo PKCS#12 (Clicar no certificado remoto correspondente e, em seguida, em exportar)
6. Importar este certificado no firewall remoto, selecionando *Deste Firewall* e, em seguida com o botão direito do mouse, *Importar*.

Na janela de requisições, há dois campos que podem causar confusão:

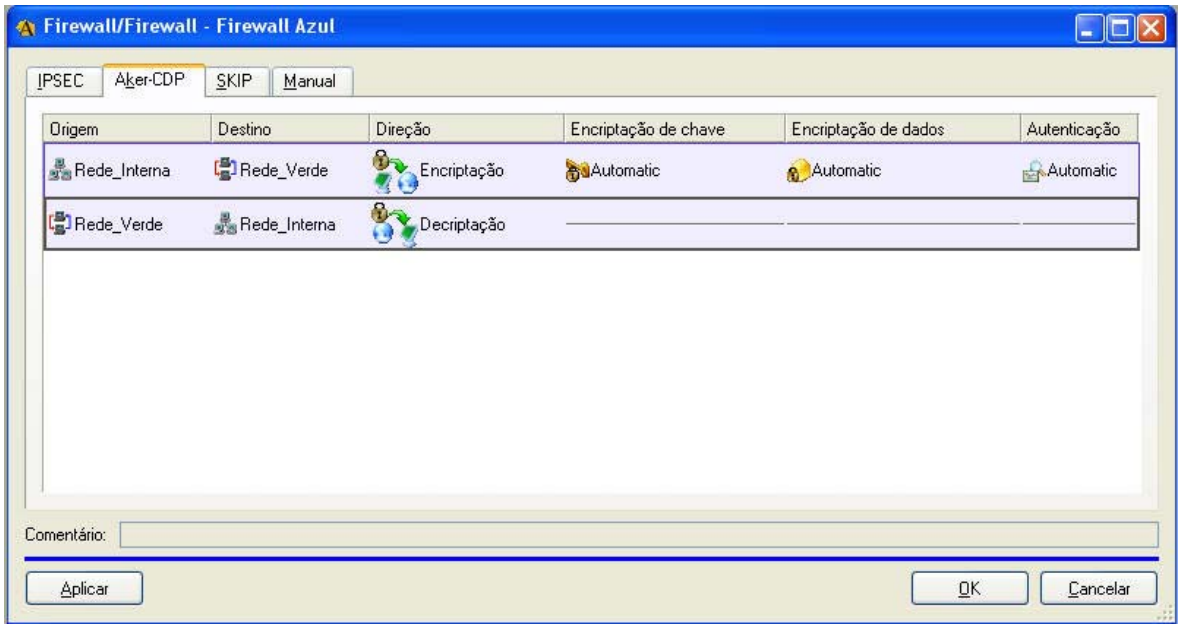
- **Dominio (CN)**: É o identificador principal do dono da requisição. Este campo deve ser preenchido com *common name.*
- **Tamanho da chave**: Se o certificado for local com criação de nova chave ou remoto, este campo conterá o comprimento da chave em bits. Caso contrário (certificado local adicional) ele não poderá ser modificado, uma vez que a chave já existente será utilizada.

8-4 Configurando canais Firewall-Firewall

Para ter acesso a janela de configuração de canais Firewall-Firewall basta:

- Clicar no menu *Criptografia* da janela principal
- Escolher o item *Firewall-Firewall*

A janela de criptografia firewall-firewall



A janela de criptografia contém a definição de todos os fluxos de criptografia do Firewall Aker. Cada fluxo será mostrado em uma linha separada, composta de diversas células. Caso um fluxo esteja selecionado, ele será mostrado em uma cor diferente. Esta janela é composta por quatro abas, onde cada uma delas permite a configuração de fluxos de criptografia usando diferentes métodos de troca de chaves.

- O botão **OK** fará com que o conjunto de fluxos seja atualizado e passe a funcionar imediatamente.

- O Botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

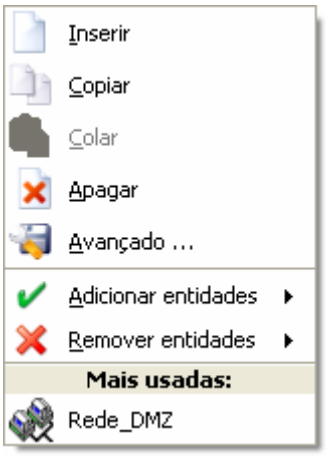
- A barra de rolagem do lado direito serve para visualizar os fluxos que não couberem na janela.
- Ao se clicar sobre um fluxo e selecioná-lo, se ele possuir um comentário, este aparecerá na parte inferior da janela.

Dica: A posição de cada regra pode ser alterada, bastando clicar e arrastar a mesma para a nova posição desejada, soltando em seguida. Observe que o cursor de indicação do mouse irá mudar para uma mão segurando um bastão.
Para se executar qualquer operação sobre um determinado fluxo, basta clicar com o botão direito do mouse sobre ele. Aparecerá o seguinte menu: (este menu será acionado sempre que se pressionar o botão direito, mesmo que não exista nenhum fluxo selecionado. Neste caso, somente as opções *Inserir* e *Colar* estarão habilitadas).

- **Inserir:** Esta opção permite se incluir um novo fluxo na lista. Se algum fluxo estiver selecionado, o novo será inserido na posição do fluxo selecionado. Caso contrário, o novo fluxo será incluído no final da lista. **Excluir**: Esta opção remove da lista o fluxo selecionado.
- **Apagar:** Esta opção apaga o fluxo selecionado.
- **Copiar:** Esta opção copia o fluxo selecionado para uma área temporária.
- **Colar:** Esta opção copia o fluxo da área temporária para a lista. Se um fluxo estiver selecionado, o novo será copiado para a posição do fluxo selecionado. Caso contrário ele será copiado para o final da lista.
- **Habilitar/Desabilitar:** Esta opção permite desabilitar o fluxo selecionado.

Dica: Todas estas opções podem ser executadas a partir da barra de ferramentas localizada na parte superior da janela. Neste caso, primeiro seleciona-se o fluxo, clicando-o com o botão esquerdo, e em seguida clica-se na opção desejada.

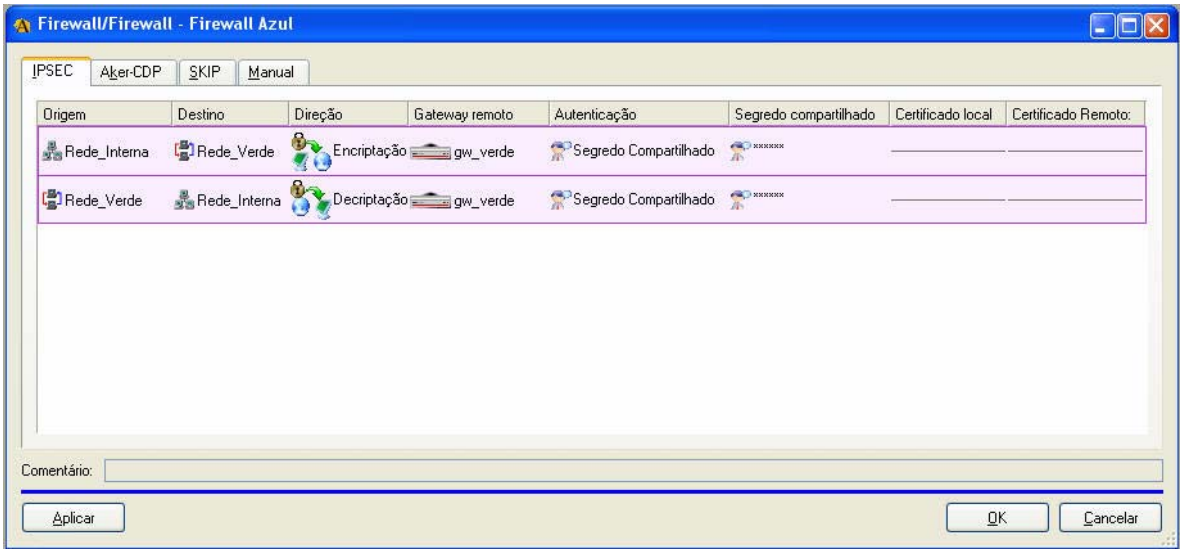
Caso deseje incluir ou editar de fluxos, pode-se fazer de duas formas: As entidades envolvidas podem ser arrastadas para o fluxo o qual vão participar ou clicando com o botão direito do mouse sobre o campo desejado, neste caso será dada a opção de inserir, apagar ou editar entidades como mostrado a seguir:.



Configurando túneis IPSEC

Túneis IPSEC servem para criar uma VPN entre duas redes. A palavra túnel é utilizada para diferenciar das VPNs comuns, pois efetivamente cria um canal virtual entre os firewalls envolvidos, possibilitando, por exemplo, que redes com endereços inválidos se comuniquem de maneira segura através da Internet.

Para se configurar canais IPSEC, deve-se selecionar a opção IPSEC, na janela Firewall-Firewall. Isto provocará a alteração da janela de forma a mostrar os campos necessários para esta configuração.



Os campos de configuração têm os seguintes significados:

Gateway Remoto: Define a entidade do tipo máquina que será o gateway remoto, ou seja, a outra ponta do túnel IPSEC.

Cada um dos dois firewalls envolvidos no túnel precisa ter certeza da identidade do outro, de forma a evitar ataques de falsificação. Para isso, há dois modos selecionáveis:

Segredo Compartilhado: Uma seqüência de caracteres que funciona como uma senha e deve ser igual de cada um dos lados do túnel.

Certificado: Utiliza certificados padrão X.509 com um esquema de chaves públicas para a identificação dos firewalls. Este É o mesmo esquema utilizado por sites seguros na Internet, por exemplo.

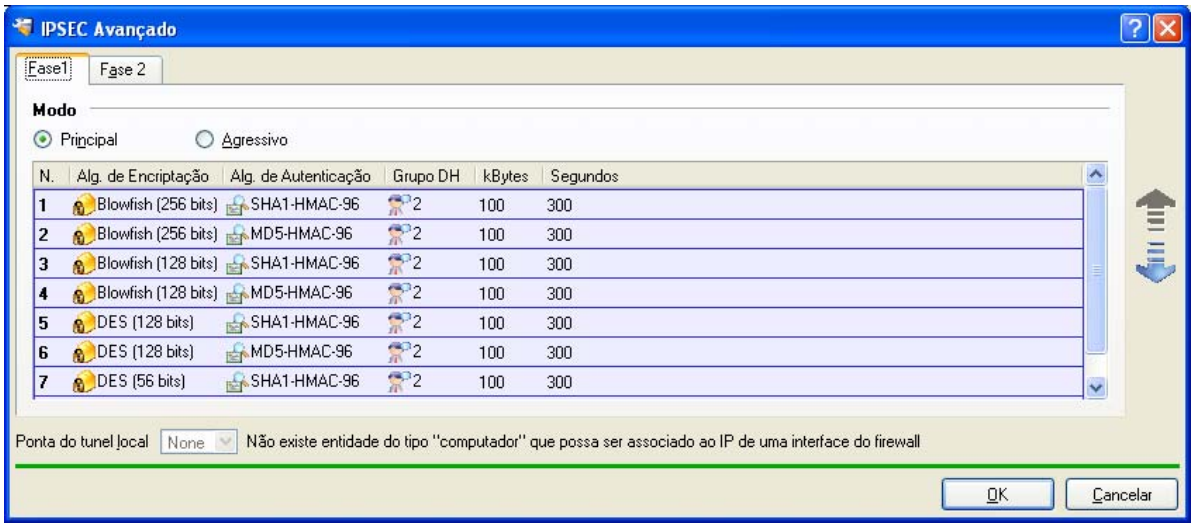
Deverão ser especificados:

- o certificado **local** a apresentar para a outra ponta do túnel (Remote Gateway) e
- o dado de identificação exigido do firewall **remoto**. Este dado será um endereço de email para certificados criados com a opção USER-FQDN e o nome de uma máquina (*Fully Qualified Domain Dame*), se a opção for FQDN.

Avançado

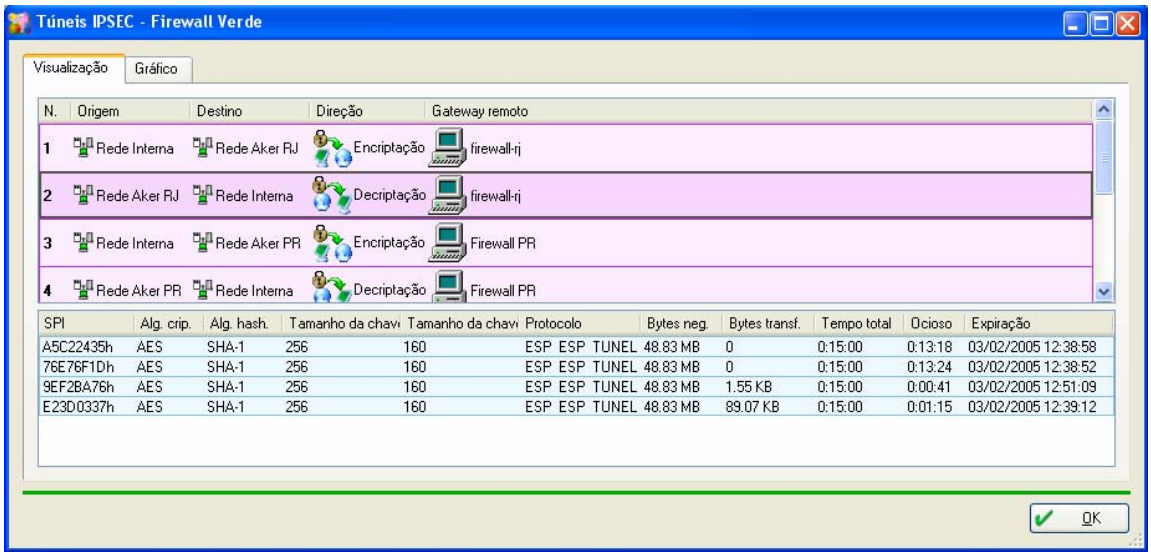
A janela avançado permite definir quais são os algoritmos de criptografia e autenticação preferidos e permitidos pelo firewall durante a negociação de chaves IKE. Os campos já vêm preenchidos com algoritmos padrão que podem ser alterados. Mais informações nas RFC 2401 a RFC 2412.

A janela de avançado agora inclui uma escolha da ponta local do túnel, para os casos da rede de passagem entre o firewall e o roteador ser inválida.


IPSEC Avançado
Fase1
Fase 2
Modo
Principal
Agressivo
N.
Alg. de Encriptação
Alg. de Autenticação
Grupo DH
kBytes
Segundos
1 Blowfish (256 bits) SHA1-HMAC-96 2 100 300
2 Blowfish (256 bits) MD5-HMAC-96 2 100 300
3 Blowfish (128 bits) SHA1-HMAC-96 2 100 300
4 Blowfish (128 bits) MD5-HMAC-96 2 100 300
5 DES (128 bits) SHA1-HMAC-96 2 100 300
6 DES (128 bits) MD5-HMAC-96 2 100 300
7 DES (56 bits) SHA1-HMAC-96 2 100 300
Ponta do tunel local
None
Não existe entidade do tipo "computador" que possa ser associado ao IP de uma interface do firewall
OK
Cancelar

Visualizando o tráfego IPSEC

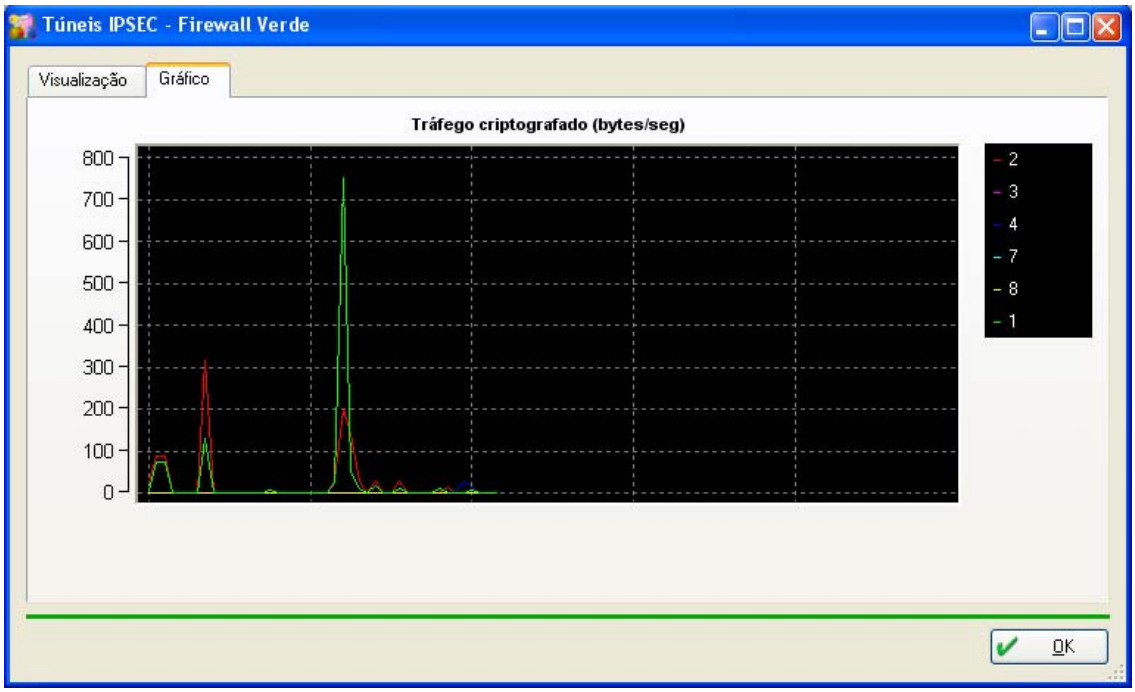
Clicando no ítem Túneis IPSEC, dentro de Informações, a janela abaixo aparecerá.


Túneis IPSEC - Firewall Verde
Visualização
Gráfico
N. Origem Destino Direção Gateway remoto
1 Rede Interna Rede Aker RJ Encriptação firewall-rj
2 Rede Aker RJ Rede Interna Decriptação firewall-rj
3 Rede Interna Rede Aker PR Encriptação Firewall PR
4 Rede Aker PR Rede Interna Decriptação Firewall PR
SPI Alg. crip. Alg. hash. Tamanho da chavi Tamanho da chavi Protocolo Bytes neg. Bytes transf. Tempo total Ocioso Expiração
A5C22435h AES SHA-1 256 160 ESP ESP TUNEL 48.83 MB 0 0:15:00 0:13:18 03/02/2005 12:38:58
76E76F1Dh AES SHA-1 256 160 ESP ESP TUNEL 48.83 MB 0 0:15:00 0:13:24 03/02/2005 12:38:52
9EF2BA76h AES SHA-1 256 160 ESP ESP TUNEL 48.83 MB 1.55 KB 0:15:00 0:00:41 03/02/2005 12:51:09
E23D0337h AES SHA-1 256 160 ESP ESP TUNEL 48.83 MB 89.07 KB 0:15:00 0:01:15 03/02/2005 12:39:12
OK

Na janela acima, é possível visualizar quais SPIs IPSEC foram negociadas para cada um dos túneis configurados, bastando para isso clicar sobre a regra correspondente. Se houver mais de uma SPI, é porque o firewall negocia uma nova sempre antes de a anterior acabar, de forma a nunca interromper o tráfego dentro da VPN. Descrição de cada coluna:

- **SPI:** Número de identificação da política de segurança
- **Algoritmo de criptografia:** Mostra que algoritmo de criptografia foi negociado
- **Algoritmo de Hash:** Mostra que algoritmo deve ser utilizado para fazer o hash das informações.
- **Tamanho da chave de criptografia:** Informa o tamanho da chave de criptografia que ambos os lados do canal devem utilizar.
- **Tamanho da chave de autenticação:** Informa o tamanho da chave de autenticação negociado.
- **Protocolo:** Conjunto de protocolos negociados para a SP
- **Bytes negociados:** Quantidade de bytes que devem ser transmitidos para que uma nova politica se segurança seja negociada.
- **Bytes transferidos:** Quantidade de bytes trafegados pela SP
- **Tempo total:** Tempo de validade da SP.
- **Ocioso:** Tempo de inatividade do SP.
- **Expiração:** Data no qual a SP deixará de ser utilizada.

Clicando-se em "gráfico", pode-se ver um gráfico de uso dos túneis, que é atualizado a cada cinco segundos. Ele mostra o tráfego agregado de todas as SPIs de cada regra, permitindo verificar, em tempo real, o uso efetivo de banda criptografada.



Utilizando a troca de chaves manual

Para se utilizar troca de chaves manual, deve-se selecionar a opção *Manual*, na janela *Firewall/Firewall*. Isto provocará a alteração da janela de forma a mostrar os campos necessários para esta configuração.

Apenas autenticação

Para se utilizar fluxos com apenas autenticação, deve-se selecionar a opção *None* no campo *Algorito de Encriptação*. Neste caso, será mostrada a seguinte janela:

Origem: Define as entidades cujos endereços serão comparados com o endereço origem dos pacotes IP que formarão o fluxo.

Destino: Define as entidades cujos endereços serão comparados com o endereço destino dos pacotes IP que formarão o fluxo.

Comentário: Reservado para se colocar um comentário sobre o fluxo. Muito útil para fins de documentação.

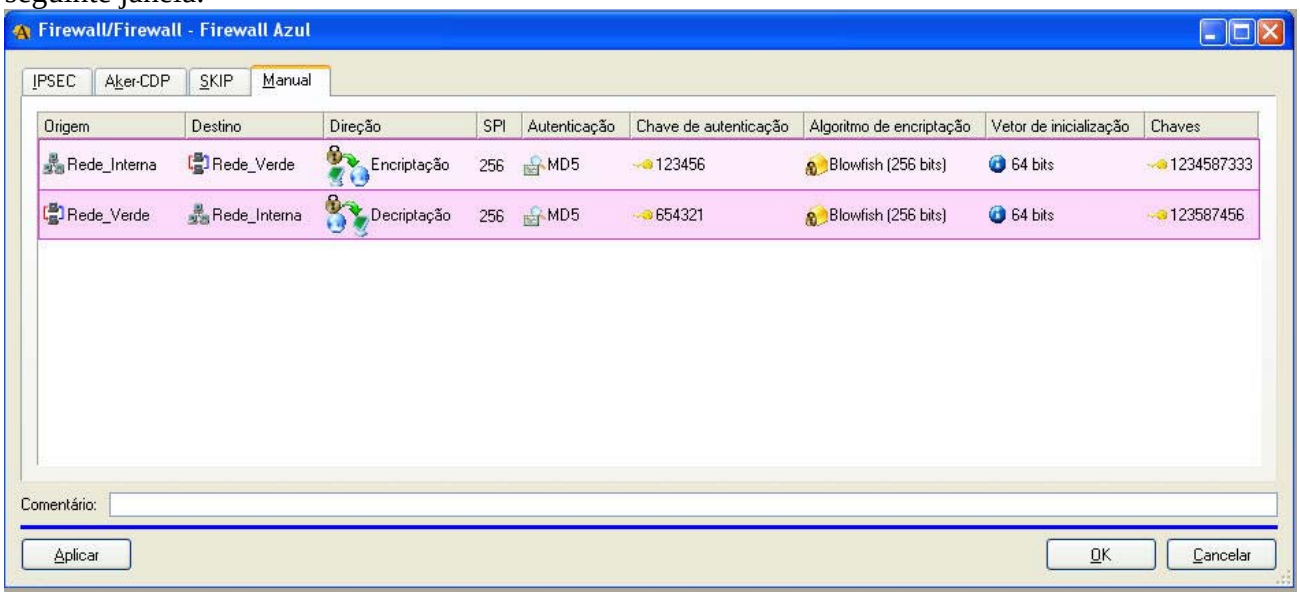
Direção: Define em que sentido o fluxo será aplicado. Só existem duas opções possíveis: ou o pacote está sendo criptografado (*encriptação*) ou o pacote esta sendo decriptado (*decriptação*). (para maiores detalhes, veja o tópico intitulado Planejando a instalação)

SPI: *(Security Parameter Index)* Este é um número único, utilizado pelo recipiente, para identificar um fluxo específico. Ele deve ser um valor maior ou igual a 256 e deve obrigatoriamente ser distinto para cada fluxo em direção a um mesmo recipiente.

Chave de Autenticação: Chave utilizada na autenticação. Esta chave deve ser digitada em hexadecimal. O seu tamanho máximo varia em função do algoritmo utilizado: 32 dígitos para o MD5 e 40 para o SHA. Recomenda-se que seja usado o número de dígitos máximo permitido.

Autenticação: Este campo define qual algoritmo de autenticação será utilizado. Os valores possíveis são: MD5 ou SHA.

Autenticação com criptografia usando o DES ou Blowfish
Para se utilizar fluxos com criptografia pelo algoritmo DES, Blowfish com chaves de 128 bits ou Blowfish com chaves de 256 bits, deve-se selecionar a opção correspondente, no campo *Algorítmo de Encriptação*. Neste caso, será mostrada a seguinte janela:

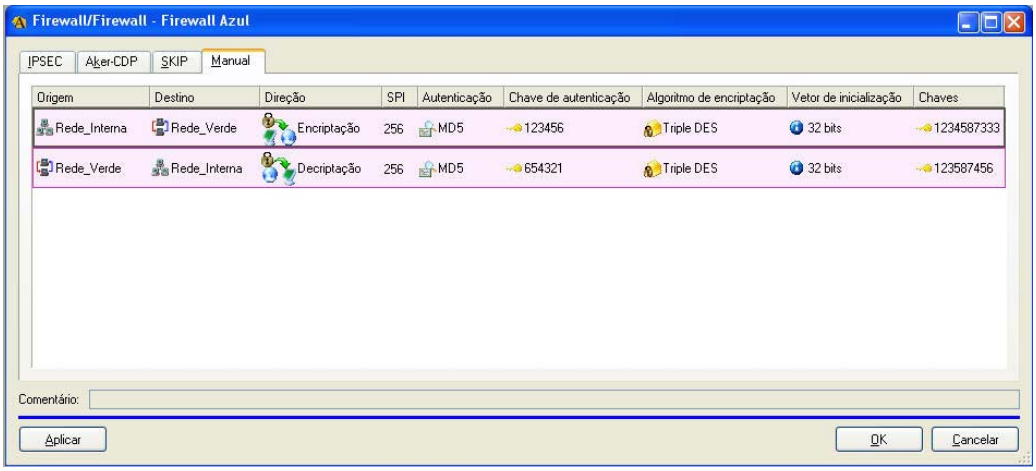


A janela mostrada neste caso é exatamente igual à do item anterior, com a exceção de dois novos campos:

Vetor de inicialização: É o tamanho, em bits, do vetor de inicialização a ser utilizado no algoritmo de criptografia. Este vetor é gerado automaticamente pelo sistema para cada pacote a ser enviado. Recomenda-se o uso da opção 64 bits.

Chaves: É a chave que será utilizada para criptografar o pacote. Ela deve ser um número hexadecimal composto obrigatoriamente de 16, 32 e 64 dígitos, no caso dos algoritmos DES, Blowfish (128 bits) e Blowfish (256 bits), respectivamente.

Autenticação com criptografia usando o Triplo DES (3DES)
Para se utilizar fluxos com criptografia pelo algoritmo Triplo DES, deve-se selecionar a opção *3DES* no campo *Algorítmo de encriptação*. Neste caso, será mostrada a seguinte janela:



A janela mostrada neste caso é exatamente igual à do item intitulado **apenas autenticação**, com alteração do campo **Chave**, onde anteriormente só havia um campo para inserção, agora são três:

Chave 1: É a chave utilizada na primeira aplicação do DES. Ela deve ser um número hexadecimal composto, obrigatoriamente, de 16 dígitos.

Chave 2: É a chave utilizada na segunda aplicação do DES. Ela deve ser um número hexadecimal composto, obrigatoriamente, de 16 dígitos.

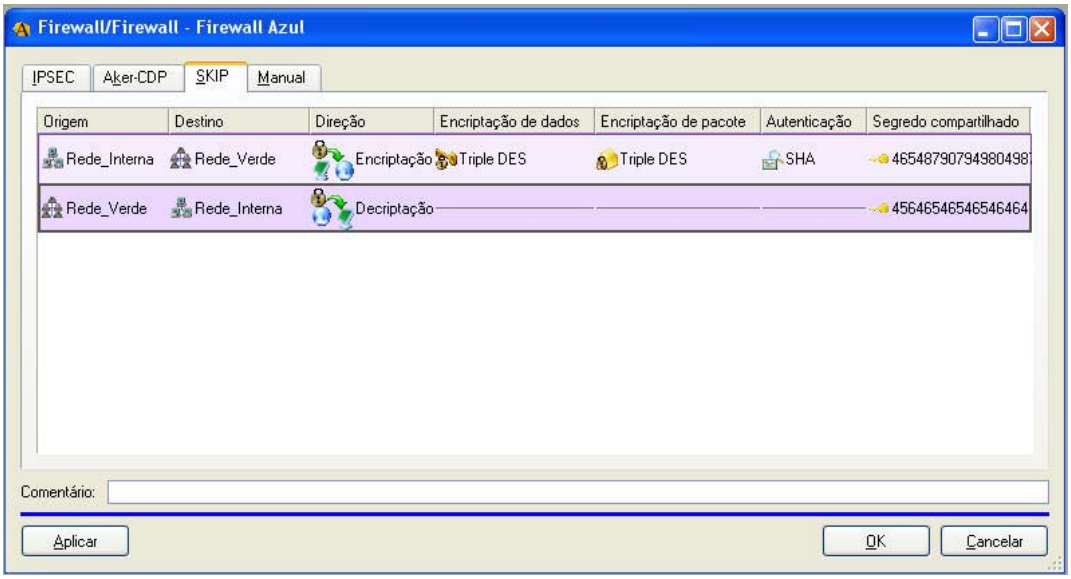
Chave 3: É a chave utilizada na terceira aplicação do DES. Ela deve ser um número hexadecimal composto, obrigatoriamente, de 16 dígitos.

Utilizando troca de chaves via SKIP

Para selecionar troca de chaves via SKIP, deve-se selecionar a opção *SKIP*, na janela *Firewall/Firewall*. Isto provocará a alteração da janela de forma a mostrar os campos necessários para esta configuração.

No protocolo SKIP, todas as informações de algoritmos de criptografia e autenticação são configurados apenas na máquina que envia os pacotes. Na máquina que irá recebê-los é necessário a configuração apenas das entidades de origem e destino e do segredo compartilhado.

Em ambos os casos será mostrada a seguinte janela: (no caso de fluxo de recebimento, os campos desnecessários estarão desabilitados)



Origem: Define as entidades cujos endereços serão comparados com o endereço origem dos pacotes IP que formarão o fluxo.

Destino: Define as entidades cujos endereços serão comparados com o endereço destino dos pacotes IP que formarão o fluxo.

Direção: Define em que sentido o fluxo será aplicado. Só existem duas opções possíveis: ou o pacote está sendo criptografado (*encriptação*) ou o pacote esta sendo decriptado (*decriptação*). (para maiores detalhes, veja o tópico intitulado Planejando a instalação)

Encriptação de dados: É o algoritmo utilizado para criptografar a chave de sessão, enviada no pacote. É aconselhável a utilização do Blowfish (256 bits).

Encriptação de pacote: É o algoritmo que será utilizado para criptografar os dados do pacote. Pode-se escolher *None* (caso se deseje utilizar apenas autenticação), *DES*, *3DES*, *Blowfish (128 bits)* ou *Blowfish (256 bits)*.

Autenticação: Define qual algoritmo será utilizado na autenticação. Os valores possíveis são: MD5 ou SHA.

Segredo Compartilhado: É o segredo que será utilizado para gerar as chaves-mestre (para maiores detalhes, veja o tópico intitulado Planejando a instalação). Este segredo deve ser o mesmo nos dois firewalls, em ambos os lados do fluxo. Ele deve ser, obrigatoriamente, um número hexadecimal com 64 dígitos.

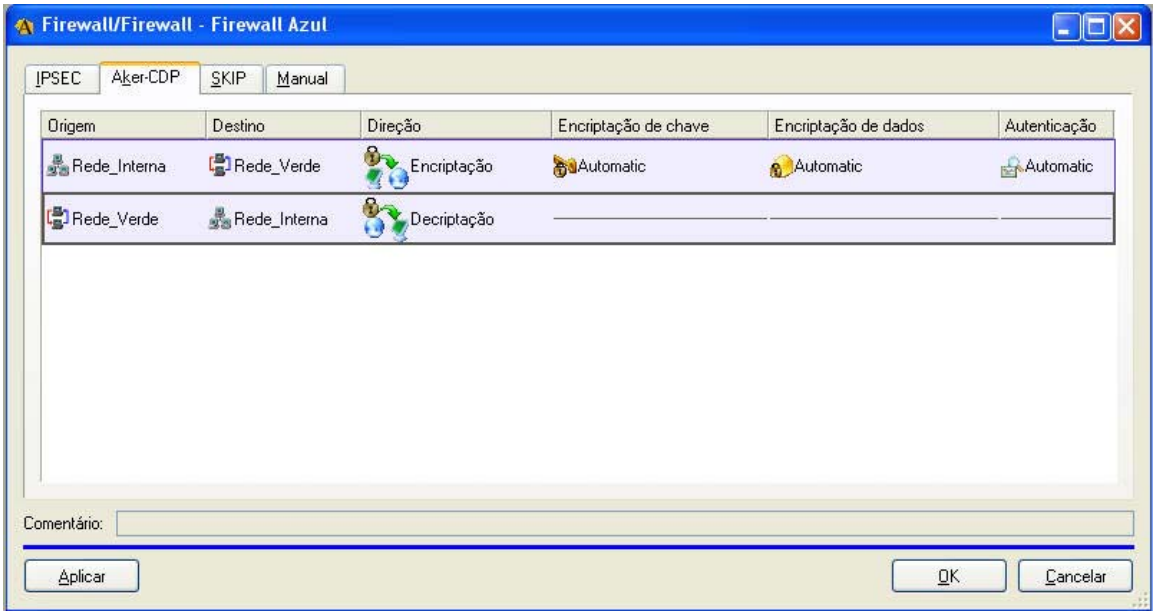
Além destes campos, existe uma opção que facilita a configuração de segredos iguais nos dois firewalls, responsáveis pela emissão e recebimento do fluxo seguro:

Carregar Segredo: Esta opção possibilita que se leia o campo *segredo compartilhado* a partir de um arquivo ASCII. Este arquivo deve possuir apenas uma linha com os 64 dígitos do segredo.

Quando esta opção for selecionada, será mostrada uma janela que possibilita a escolha do nome do arquivo onde será lido o segredo.

Utilizando troca de chaves via Aker-CDP

Para selecionar troca de chaves via Aker-CDP, deve-se selecionar a opção *Aker-CDP*, na janela *Firewall/Firewall*. Isto provocará a alteração da janela de forma a mostrar os campos necessários para esta configuração. Ela terá o seguinte formato:



A configuração dos parâmetros da troca de chaves via Aker-CDP é idêntica a da troca de chaves via SKIP, mostrada anteriormente, exceto pelo fato de que não é necessário se especificar um segredo compartilhado e todos os algoritmos podem ser deixados na opção *Automática*, o que fará com que os firewalls participantes do canal negociem o algoritmo mais seguro suportado por ambos.

8-5 Utilizando a interface texto

Através da interface texto, é possível se realizar todas as configurações mostradas acima. A descrição de cada configuração distinta se encontra em um tópico separado.

Carregando certificados IPSEC

A interface texto de configuração dos certificados IPSEC é de uso simples e possui as mesmas capacidades da interface gráfica.
Localização do programa: `/etc/firewall/fwipseccert`

Sintaxe:

```
Uso: fwipseccert ajuda
     fwipseccert mostra [requisicao | certificado]
     fwipseccert remove [requisicao | certificado] <numero>
     fwipseccert requisita <local | remoto> <1024 | 2048> <email>
<pais> <estado>
            <cidade> <organizacao> <unid org> <dominio>
            [use_email] [imprime]
     fwipseccert instala <local | remoto> <certificado>
     fwipseccert exporta <certificado> <arquivo PKCS12> <senha>
     fwipseccert importa <arquivo PKCS12> <senha>
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
fwipseccert - Criacao e manejamento de requisicoes e certificados
x.509
Uso: fwipseccert ajuda
     fwipseccert mostra [requisicao | certificado]
     fwipseccert remove [requisicao | certificado] <numero>
     fwipseccert requisita <local | remoto> <1024 | 2048> <email>
<pais> <estado>
            <cidade> <organizacao> <unid org> <dominio>
            [use_email] [imprime]
     fwipseccert instala <local | remoto> <certificado>
     fwipseccert exporta <certificado> <arquivo PKCS12> <senha>
     fwipseccert importa <arquivo PKCS12> <senha>

     ajuda      = mostra esta mensagem
     mostra     = mostra uma lista contendo as requisicoes pendentes
ou os
                  certificados instalados
     remove     = remove uma requisicao ou certificado de acordo com
seu numero
     requisita  = cria um par de chaves publicas e privadas juntamente
com uma
                  requisicao de um certificado x.509
     instala    = instala um certificado x.509 cujo o par de chaves
deve ter
                  sido criado anteriormente pelo sistema atraves do
comando
                  requisita
     exporta    = exporta o certificado e seu par de chaves
correspondente para
                  para um arquivo de formato pkcs12
     importa    = obtem do arquivo pkcs12 um certificado e seu par de
chaves e o
                  instala como certificado local(ver abaixo)

Para requisita temos:
     local      = o certificado local e' usado na indentificacao do
proprio
                  firewall; pode-se criar varios certificados locais
porem,
                  todos eles usarao o mesmo par de chaves que e'
gerado na
                  primeira vez que uma requisicao local e' gerada
     remoto     = certificados remotos sao utilizados para
identificacao de
                  outras entidades da rede.
     1024/2048  = sao os possiveis tamanhos das chaves que serao
geradas
     use_email  = o certificado contera o valor de <email> como seu
subject
                  alternative name; como default ele usara o valor de
<dominio>
     imprime    = apos a criacao da requizicao, ela sera impressa na
tela

     email, pais, estado, cidade, organizacao, unid org e dominio sao
campos que
              serao usados para indentificar do usuario do certificao.
O campo
```

```
            <pais> deve conter 2 caracteres no maximo. O campo <unid
org> e'
            abreviatura de unidade organizacional e se refere ao
departamento
            ou divisao da organizacao ao qual pertence o usuario do
certificado
```

Carregando certificados

A interface texto de configuração dos certificados de criptografia é de uso simples e possui as mesmas capacidades da interface gráfica.
Localização do programa: `/etc/firewall/fwcert`

Sintaxe:

```
fwcert ajuda
fwcert mostra [local | ca | negociacao | revogacao]
fwcert carrega [local | ca] <arquivo> [-f]
fwcert carrega revogacao <arquivo>
fwcert remove <codigo> [-f]
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
fwcert - Configura os certificados para criptografia
Uso: fwcert ajuda
     fwcert mostra [local | ca | negociacao | revogacao]
     fwcert carrega [local | ca] <arquivo> [-f]
     fwcert carrega revogacao <arquivo>
     fwcert remove <codigo> [-f]

     ajuda      = mostra esta mensagem
     mostra     = mostra os certificados especificados
     carrega    = carrega um novo certificado no firewall
     remove     = remove o certificado de uma entidade certificadora

Para mostra temos:
     local      = mostra o certificado de negociacao local
     ca         = mostra os certificados das entidades certificadoras
     negociacao = mostra os certificados de negociacao de outros
firewalls
                  que foram recebidos pela rede
     revogacao  = mostra os certificados de revogacao que foram
carregados
                  localmente ou recebidos pela rede

Para carrega temos:
     local      = carrega o certificado de negociacao local (se ja
existir um
                  certificado carregado ele sera substituido)
     ca         = carrega um certificado de uma Entidade Certificadora
que sera
                  usado para validar os certificados de negociacao
recebidos
                  (se ja existir um outro certificado com o mesmo
codigo ele
                   sera substituido)
     revogacao  = carrega um certificado de revogacao, que sera usado
para
                  invalidar um certificado de negociacao comprometido
     arquivo    = nome do arquivo do qual o certificado sera carregado
```

```
     -f         = se estiver presente, faz com que o programa nao
confirme ao
                  substituir um certificado

Para remove temos:
     codigo     = codigo da entidade certificadora a ser removida
     -f         = se estiver presente, faz com que o programa nao
confirme ao
                  remover um certificado
```

Exemplo 1: (carregando o certificado local)

```
#/etc/firewall/fwcert carrega local /tmp/firewall.crt
Carregando certificado...OK
```

Exemplo 2: (mostrando os certificados de entidades certificadoras)

```
#/etc/firewall/fwcert mostra ca
Nome: Aker Security Solutions
Codigo: 1

Nome: Entidade certificadora autorizada
Codigo: 2
```

Exemplo 3: (carregando um novo certificado de entidade certificadora)

```
#/etc/firewall/fwcert carrega ca /tmp/novo_ca.ca
Certificado incluido
```

Exemplo 4: (removendo um certificado de entidade certificadora, sem confirmação)

```
#/etc/firewall/fwcert remove 2 -f
Entidade certificadora removida
```

Configurando canais Firewall-Firewall

A utilização da interface texto na configuração das regras de criptografia e de autenticação firewall-firewall traz uma dificuldade gerada pela grande quantidade de parâmetros que devem ser passados na linha de comando.

Esta interface texto possui as mesmas capacidades da interface gráfica com a exceção de que através dela não é possível se atribuir comentários para os canais seguros, se especificar mais de uma entidade como origem ou destino deles nem atribuir algoritmos para troca de chaves via Aker-CDP (neste caso, os algoritmos serão sempre marcados com a opção de negociação automática). Além disso, não será possível configurar os algoritmos a serem usados pelo IPSEC-IKE (janela avançado), eles terão sempre os valores padrão.

Localização do programa: `/etc/firewall/fwcripto`

Sintaxe:

```
Uso: fwcripto [mostra | ajuda]
     fwcripto [habilita | desabilita | remove] <pos>
     fwcripto inclui <pos> <origem> <destino> <envia | recebe>
              ipsec <gateway> <ss <segredo> | cert <local> <remoto>>
     fwcripto inclui <pos> <origem> <destino> <envia | recebe>
              manual <spi> <MD5 | SHA> <chave autenticacao> NENHUM
     fwcripto inclui <pos> <origem> <destino> <envia | recebe>
              manual <spi> <MD5 | SHA> <chave autenticacao>
              <DES | BFISH128 | BFISH256> <tamanho_iv> <chave
criptografia>
     fwcripto inclui <pos> <origem> <destino> <envia | recebe>
              manual <spi> <MD5 | SHA> <chave autenticacao>
```

```
               3DES <tamanho_iv> <chave1> <chave2> <chave3>
     fwcripto inclui <pos> <origem> <destino> envia
               skip <DES | 3DES | BFISH256> <MD5 | SHA>
               <NENHUM | DES | 3DES | BFISH128 | BFISH256> <segredo>
     fwcripto inclui <pos> <origem> <destino> recebe
               skip <segredo>
     fwcripto inclui <pos> <origem> <destino> <envia | recebe> aker-
cdp
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
fwcripto - Configura a tabela de autenticacao e criptografia
Uso: fwcripto [mostra | ajuda]
     fwcripto [habilita | desabilita | remove] <pos>
     fwcripto inclui <pos> <origem> <destino> <envia | recebe>
               ipsec <gateway> <ss <segredo> | cert <local> <remoto>>
     fwcripto inclui <pos> <origem> <destino> <envia | recebe>
               manual <spi> <MD5 | SHA> <chave autenticacao> NENHUM
     fwcripto inclui <pos> <origem> <destino> <envia | recebe>
               manual <spi> <MD5 | SHA> <chave autenticacao>
               <DES | BFISH128 | BFISH256> <tamanho_iv> <chave
criptografia>
     fwcripto inclui <pos> <origem> <destino> <envia | recebe>
               manual <spi> <MD5 | SHA> <chave autenticacao>
               3DES <tamanho_iv> <chave1> <chave2> <chave3>
     fwcripto inclui <pos> <origem> <destino> envia
               skip <DES | 3DES | BFISH256> <MD5 | SHA>
               <NENHUM | DES | 3DES | BFISH128 | BFISH256> <segredo>
     fwcripto inclui <pos> <origem> <destino> recebe
               skip <segredo>
     fwcripto inclui <pos> <origem> <destino> <envia | recebe> aker-
cdp

     mostra     = mostra todas as entradas da tabela de criptografia
     inclui     = inclui uma entrada na tabela
     habilita   = habilita uma entrada previamente desabilitada
     desabilita = desabilita uma entrada existente
     remove     = remove uma entrada existente da tabela
     ajuda      = mostra esta mensagem

Para inclui temos:
     pos        = posicao onde a nova entrada sera incluida na tabela
                  (Podera ser um inteiro positivo ou a palavra FIM
                   para incluir no final da tabela)
     envia      = esta entrada sera usada na hora de enviar pacotes
     recebe     = esta entrada sera usada na hora de receber pacotes
     ipsec      = usa troca de chave e protocolo IPSEC
     gateway    = a entidade que representa a ponta remota do tunel
IPSEC
     ss         = usa segredo compartilhado como forma de autenticacao
     segredp    = a "string" que sera usada como segredo compartilhado
     cert       = usa certificados X.509 para autenticacao
     local      = o nome de dominio (FQDN) no certificado a apresentar
     remoto     = o nome de dominio (FQDN) no certificado esperado
     manual     = utiliza troca de chaves manual
     skip       = utiliza troca de chaves automatica via o protocolo
SKIP
     aker-cdp   = utiliza troca de chaves automatica via o protocolo
Aker-CDP
     spi        = indice de parametro de seguranca
                  (E' um inteiro que identifica unicamente a
associacao de
```

```
                  seguranca entre a maquina de origem e de destino.
Este
                  numero deve ser maior que 255)
     MD5        = usa como algoritmo de autenticacao o MD5
     SHA        = usa como algoritmo de autenticacao o SHA-1
     DES        = usa como algoritmo de criptografia o DES
     3DES       = usa como algoritmo de criptografia o triplo DES
     BFISH128   = usa como algoritmo de criptografia o Blowfish com
chaves de
                  128 bits
     BFISH256   = usa como algoritmo de criptografia o Blowfish com
chaves de
                  256 bits
     NENHUM     = nao usa criptografia, somente autenticacao
                  (No caso do skip, o primeiro algoritmo selecionado
                   correponde ao algoritmo de criptografia da chave e
                   o segundo corresponde ao de criptografia do pacote)
     tamanho_iv = tamanho do vetor de inicializacao, em bits, para o
algoritmo
                  de criptografia. Deve ter o valor 32 ou 64.

     As chaves de autenticacao, criptografia e o segredo skip
     devem ser entradas como numeros hexadecimais.
     No caso do 3DES devem ser digitadas 3 chaves separadas por
brancos

Para habilita / desabilita / remove temos:
     pos        = posicao a ser habilitada, desabilitada ou removida
da tabela
                  (a posicao e' o valor mostrado na esquerda da
entrada ao
                   se usar a opcao mostra)
```

Exemplo 1: (mostrando a tabela de criptografia)

```
#/etc/firewall/fwcripto mostra
Entrada 01:
----------
Origem       : REDE1
Destino      : AKER
Sentido      : Recebe   Chaves: SKIP
Segredo      :
5ab53faefc7c9845acbe223148065dabe3279819ab01c39654effacbef087022

Entrada 02:
----------
Origem       : AKER
Destino      : REDE1
Sentido      : Envia    Chaves: SKIP           Algoritmos: 3DES MD5
DES
Segredo      :
5ab53faefc7c9845acbe223148065dabe3279819ab01c39654effacbef087021

Entrada 03:
----------
Origem       : Rede Interna
Destino      : Rede externa 1
Sentido      : Envia    Chaves: Manual         Algoritmos: SHA DES
SPI          : 999      Autenticacao: 0c234da5677ab5
Criptografia : 9a34ac7890ab67ef
VI: 64 bits

Entrada 04:
```

```
----------
Origem       : Rede externa 1
Destino      : Rede Interna
Sentido      : Recebe   Chaves: Manual         Algoritmos: SHA DES
SPI          : 999      Autenticacao: 0c234da5677ab5
Criptografia : 9a3456ac90ab67ef
VI: 64 bits

Entrada 05:
----------
Origem       : Rede Aker 1
Destino      : Rede Aker 2
Sentido      : Recebe   Chaves: Aker-CDP      Algoritmos: Auto Auto
Auto

Entrada 06:
----------
Origem       : Rede Aker 2
Destino      : Rede Aker 1
Sentido      : Envia    Chaves: Aker-CDP      Algoritmos: Auto Auto
Auto
```

Exemplo 2: (removendo a terceira entrada da tabela)

```
#/etc/firewall/fwcripto remove 3
Entrada 3 removida
```

Exemplo 3: (incluindo uma entrada com troca de chaves manual e criptografia via DES no final da tabela)

```
#/etc/firewall/fwcripto inclui fim REDE1 REDE2 envia manual 7436 MD5
c234da5677ab5 DES 64 4234ad70cba32c6ef
Entrada incluida na posicao 7
```

Exemplo 4: (incluindo uma entrada com troca de chaves via SKIP no inicio da tabela)

```
#/etc/firewall/fwcripto inclui 1 Rede1 Rede2 envia skip 3DES SHA DES
5ab53faefc7c9845acbe223148065dabe3279819ab01c39654effacbef087022
Entrada incluida na posicao 1
```

Exemplo 5: (incluindo uma entrada com troca de chaves via Aker-CDP na posicao 2 da tabela)

```
# /etc/firewall/fwcripto inclui 2 "Rede Aker 3" "Rede Aker 1" recebe
aker-cdp
Entrada incluida na posicao 2
```

9-0 Configurando Criptografia Cliente-Firewall

Mostraremos aqui como configurar o firewall e o cliente de criptografia Aker de modo a propiciar a criação de canais seguros entre máquinas clientes e um Firewall Aker.

9-1 Planejando a instalação.

O que é um canal seguro Cliente-Firewall?

Conforme já explicado no capítulo anterior, um canal seguro cliente-firewall é aquele estabelecido diretamente entre uma máquina cliente e um Firewall Aker. Isto é possível com a instalação de um programa, chamado de Cliente de Criptografia Aker, nas máquinas clientes.

Um canal de criptografia Cliente-Firewall utiliza as mesmas tecnologias de criptografia, autenticação e troca de chaves já mostradas para os canais seguros Firewall-Firewall, com a diferença de que tudo é negociado automaticamente pelas partes comunicantes. Ao administrador, é possível apenas desabilitar determinados algoritmos, de forma a assegurar que eles não serão utilizados.

Outra diferença fundamental entre os canais seguros firewall-firewall e cliente-firewall, da forma com que são implementados no Firewall Aker, é que os primeiros são sempre realizados ao nível de pacotes IP, onde cada pacote é encriptado individualmente, enquanto que os segundos são feitos ao nível de fluxo de dados, encriptado somente as informações contidas na comunicação (e não os demais dados do pacote IP).

Exigências para a criação de canais seguros Cliente-Firewall

Para que seja possível o estabelecimento de canais seguros entre clientes e um firewall, é necessário que a seguinte lista de condições seja atendida:

1. O Cliente de Criptografia Aker esteja instalado em todas as máquinas que estabelecerão canais seguros com o firewall
2. O certificado local do firewall esteja carregado (para maiores informações sobre certificados, veja o capítulo entitulado Criando canais de criptografia)
3. O firewall esteja configurado de forma a permitir que clientes de criptografia estabeleçam sessões seguras
4. Os clientes estejam configurados de forma a estabelecer canais de criptografia com as redes protegidas pelo firewall

O cliente de criptografia utilizará a porta 2473/UDP (protocolo Aker-CDP) para estabelecer o canal seguro com o firewall. É necessário que não exista nenhum outro

firewall ou mecanismo de controle no caminho que impeça a passagem de pacotes para esta porta, caso contrário não será possível o estabelecimento dos canais seguros.

O cliente de criptografia somente encripta dados enviados através de Winsock, não encriptando nenhum tipo de comunicação NetBIOS.

Definindo um canal seguro cliente-firewall

A definição de um canal seguro cliente-firewall é bem mais simples do que a de um canal firewall-firewall. É necessário apenas se configurar no firewall quais máquinas poderão estabelecer canais seguros de clientes e se ocorrerá ou não autenticação de usuários. Todo o restante da configuração é feito automaticamente, no momento em que o cliente inicia a abertura do canal seguro.

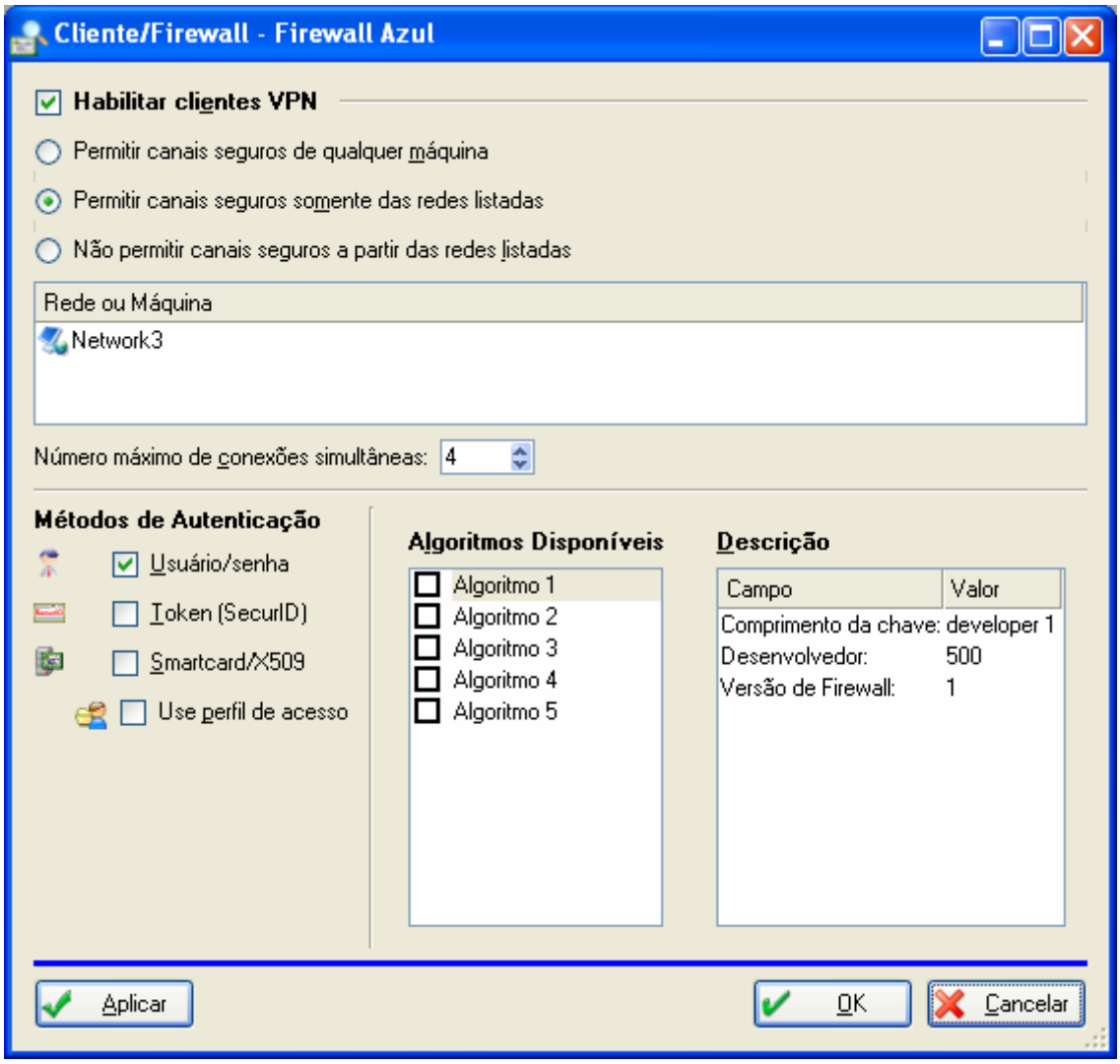
9-2 Configurando o Firewall utilizando a interface gráfica

A configuração dos canais cliente-firewall é bastante simples, uma vez que todo o procedimento é feito automaticamente pelo cliente e pelo firewall. Ao administrador cabe apenas definir quais clientes podem estabelecer um canal seguro e se será realizada autenticação de usuários.

Todas estas configurações são feitas na janela de canais seguros de clientes. Para acessá-la, basta:

- Clicar no menu *Criptografia* da janela principal
- Escolher o item *Cliente/Firewall*

A janela de criptografia cliente-firewall



Os parâmetros de configuração de canais cliente são formados pelos seguintes campos:

Habilitar clientes VPN: Esta opção deve ser marcada para ativar o suporte no firewall para os canais seguros de clientes. Ao se desabilitar o suporte a clientes de criptografia, a configuração continuará armazenada, mas não poderá ser alterada.

Permitir canais seguros de qualquer máquina: Esta opção permite que qualquer máquina na Internet estabeleça um canal seguro com o Firewall.

Permitir canais seguros apenas das redes listadas: Esta opção exige que qualquer entidade que queira estabelecer um canal seguro esteja presente na lista logo abaixo.

Não permitir canais seguros das redes listadas: Esta opção é oposta à anterior e exige que as entidades que queiram estabelecer um canal seguro não estejam presentes na lista logo abaixo.

Adicionando e removendo entidades da lista de entidades (exceto se *Permitir canais seguros de qualquer máquina* estiver marcado):

Para se adicionar uma entidade à lista, deve-se proceder da seguinte forma:

- Clique com o botão direito do mouse no campo onde a entidade será inserida, ou
- arraste a entidades do campo entidades, localizado no lado inferior esquerdo, para cima do campo desejado.

Para se remover uma entidade, deve-se proceder da seguinte forma:

- Clica-se com o botão direito do mouse no campo de onde a entidade será removida.

Número máximo de conexões simultâneas: Este parâmetro configura o número máximo de canais seguros de clientes que podem estar ativos em um determinado instante. Ele pode variar entre 0 e o número máximo de licenças de clientes de criptografia adquiridas. Se estiver em 0, não será permitido a nenhum usuário estabelecer canais seguros.

Métodos de Autenticação

As opções disponíveis, que podem ser marcadas independentemente, são:

- Usuário/senha

O usuário deverá se autenticar através de uma combinação de nome e uma senha. Esses dados serão repassados a um ou mais servidores de autenticação que deverão validá-los. Esta opção é a mais insegura porém não depende de nenhum hardware adicional.

- Token (SecurID)

O usuário deverá se autenticar mediante o fornecimento de um nome, um PIN e um código presente em um Token SecurID que é modificado a cada minuto. Esses dados serão repassados para o autenticador Token cadastrado no firewall para serem validados. Essa opção é bem mais segura que a anterior, porém exige que cada usuário possua um Token.

- Smart Card

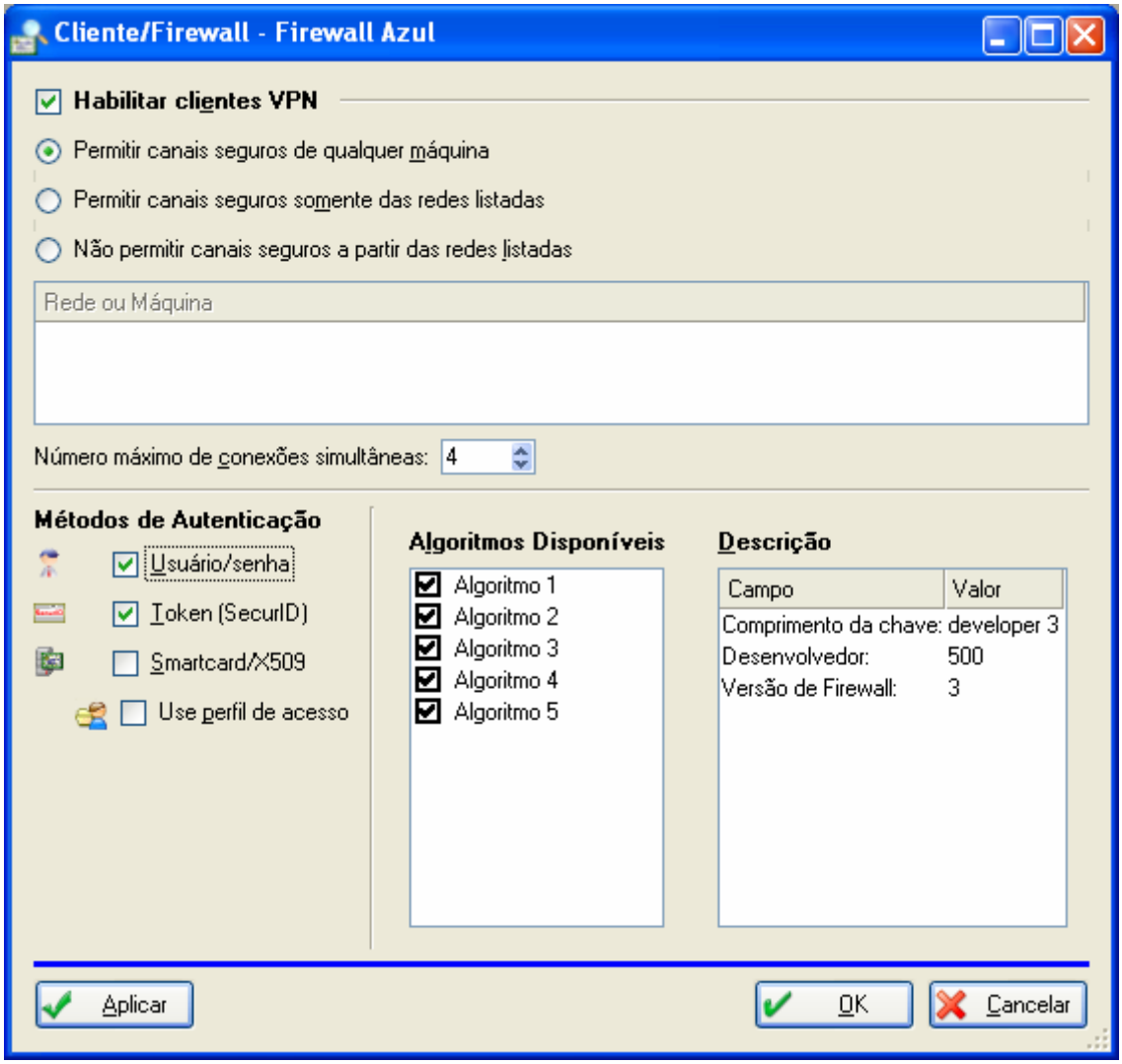
O usuário deverá se autenticar através do uso de certificados X509 (por exemplo, gravados em smart cards) e emitidos por uma das autoridades certificadoras cadastradas no firewall. Essa forma de autenticação é a mais segura das três, pois exigir a senha de desbloqueio da chave privada e a posse da mesma.
Caso alguma opção em *Métodos de Autenticação* esteja marcada, é possível se definir se um usuário validado no cliente de criptografia terá ou não um perfil de acesso associado a ele. Se a opção **Utiliza perfil de acesso** esteja marcada, então ao ser validado no cliente de criptografia o usuário terá os mesmos direitos que teria caso se autenticasse também através do cliente de autenticação. Caso esta opção esteja desmarcada, então o usuário estabelecerá um canal seguro porém não terá nenhum perfil de acesso associado a ele (esse último é o comportamento da versão 3.52 e anteriores do firewall).

É possível se utilizar o Cliente de Autenticação Aker em conjunto com o cliente de criptografia. Desta forma, caso se esteja utilizando autenticação por usuário/senha, não é

necessário ao usuário se autenticar novamente para o firewall. Para maiores informações sobre o cliente de autenticação veja o capítulo intitulado O cliente de autenticação Aker.

Habilitando e desabilitando algoritmos de criptografia

É possível para o administrador desabilitar algoritmos de criptografia, de modo a impedir que estes sejam utilizados em canais seguros cliente/firewall. Para se fazer isso basta desmarcar a check box correspondente ao algorítmo, no campo **Algoritmos Disponíveis**, localizado na parte inferior da janela de criptografia cliente/firewall.



9-3 Configurando o Firewall utilizando a interface texto

A interface texto de configuração de canais seguros Cliente-Firewall é de uso simples e possui as mesmas capacidades da interface gráfica.
Localização do programa: `/etc/firewall/fwclient`

Sintaxe:

```
fwclient [ativa | desativa | mostra | ajuda]
fwclient [inclui | remove] <nome>
fwclient [habilita | desabilita] <algoritmo>
```

```
fwclient max_clientes <valor>
fwclient autenticacao nenhuma
fwclient autenticacao [senha | cartao | token] <sim | nao>
fwclient permite [todos | listados | outros]
fwclient perfil <sim | nao>
```

Ajuda do programa:

```
Firewall Aker - Versao 5.0
fwclient - Configura parametros de canais seguros para clientes
Uso: fwclient [ativa | desativa | mostra | ajuda]
     fwclient [inclui | remove] <nome>
     fwclient [habilita | desabilita] <algoritmo>
     fwclient max_clientes <valor>
     fwclient autenticacao nenhuma
     fwclient autenticacao [senha | cartao | token] <sim | nao>
     fwclient permite [todos | listados | outros]
     fwclient perfil <sim | nao>

     ativa        = ativa suporte a canais seguros para clientes
     desativa     = desativa suporte a canais seguros para clientes
     mostra       = mostra a configuracao atual
     inclui       = inclui uma entidade na lista de entidades
     remove       = remove uma das entidades da lista de entidades
     habilita     = habilita o uso do algoritmo especificado
     desabilita   = desabilita o uso do algoritmos especificado
     max_clientes = configura o numero maximo de clientes simultaneos
     autenticacao = desativa ou seleciona os tipos de autenticacao de
usuarios
                    que serao aceitos para maquinas clientes
estabelecerem
                    canais seguros
     permite      = indica quais entidades poderao estabelecer canais
seguros
                    com o firewall
     perfil       = Habilita o uso de perfis de acesso para usuarios
validados
                    pelo cliente de criptografia
     ajuda        = mostra esta mensagem

Para inclui / remove temos:
     nome         = nome da entidade a ser incluida ou removida da
lista

Para max_clientes temos:
     valor        = numero maximo de clientes simultaneos (deve ser um
numero
                    inteiro entre 0 e 1000)

Para autenticacao temos:
     nenhuma      = nao exige autenticacao de usuarios
     senha        = aceita ou nao autenticacao por usuario/senha
     cartao       = aceita ou nao autenticacao por smart card
     token        = aceita ou nao autenticacao por tokens

Para permite temos:
     todos        = permite que qualquer maquina na Internet
estabeleca um
                    canal seguro com o firewall
     listados     = permite apenas as maquinas, redes ou conjuntos
listados
                    estabelecer canais seguros com o firewall
     outros       = permite a todas as maquinas na Internet menos as
```

```
maquinas,
                    redes ou conjuntos listados estabelecerem canais
seguros
                    com o firewall
```

Exemplo 1: (mostrando a configuração)

```
#/etc/firewall/fwclient mostra
Parametros de configuracao:
---------------------------
Suporte a canais seguros para clientes: ativado
Numero maximo de clientes simultaneos : 25
Utiliza perfis de acesso: sim
Autenticacao de usuarios: nenhuma

NAO permite canais seguros apenas para as entidades abaixo:
-----------------------------------------------------------
hacker1                                          (Maquina)
rede teste                                       (Rede)

Algoritmos carregados:
----------------------
DES                                              (habilitado)
3-DES                                            (habilitado)
Blowfish-128                                     (habilitado)
Blowfish-256                                     (habilitado)
```

Exemplo 2: (ativando a autenticação de usuários por usuário senha e mostrando a nova configuração)

```
#/etc/firewall/fwclient autenticacao senha sim
#/etc/firewall/fwclient mostra
Parametros de configuracao:
---------------------------
Suporte a canais seguros para clientes: ativado
Numero maximo de clientes simultaneos : 25
Utiliza perfis de acesso: sim
Autenticacao de usuarios:
   Usuario/senha: sim
   Smart card   : nao
   Token        : nao

NAO permite canais seguros apenas das entidades abaixo:
-------------------------------------------------------
hacker1                                          (Maquina)
rede teste                                       (Rede)

Algoritmos carregados:
----------------------
DES                                              (habilitado)
3-DES                                            (habilitado)
Blowfish-128                                     (habilitado)
Blowfish-256                                     (habilitado)
```

Exemplo 3: (permitindo o estabelecimento de canais seguros de qualquer máquina e mostrando a nova configuração)

```
#/etc/firewall/fwclient permite todos
#/etc/firewall/fwclient mostra
Parametros de configuracao:
---------------------------
Suporte a canais seguros para clientes: ativado
Numero maximo de clientes simultaneos : 25
Utiliza perfis de acesso: sim
Autenticacao de usuarios:
   Usuario/senha: sim
```

```
   Smart card   : nao
   Token        : nao

Permite canais seguros de qualquer maquina da Internet

Algoritmos carregados:
----------------------
DES                                                (habilitado)
3-DES                                              (habilitado)
Blowfish-128                                       (habilitado)
Blowfish-256                                       (habilitado)
```

Exemplo 4: (desabilitando o algoritmo DES e mostrando a nova configuração)

```
#/etc/firewall/fwclient desabilita des
#/etc/firewall/fwclient mostra
Parametros de configuracao:
---------------------------
Suporte a canais seguros para clientes: ativado
Numero maximo de clientes simultaneos : 25
Utiliza perfis de acesso: sim
Autenticacao de usuarios:
   Usuario/senha: sim
   Smart card   : nao
   Token        : nao

Permite canais seguros de qualquer maquina da Internet

Algoritmos carregados:
----------------------
DES                                                (desabilitado)
3-DES                                              (habilitado)
Blowfish-128                                       (habilitado)
Blowfish-256                                       (habilitado)
```

9-4 Instalando o Cliente de Criptografia Aker

O Cliente de Criptografia Aker funciona em plataformas Windows 95/98/NT/2000. Sua instalação é bastante simples e não é necessário nem a reinicialização da máquina onde ele será instalado.

Para instalar o cliente de criptografia deve-se colocar o CD-ROM no drive e selecionar a opção **Instalar Cliente de Criptografia**, dentro do menu **Firewall,** na janela de apresentação. Caso a opção de auto-execução esteja desabilitada, então é necessário se executar os seguintes passos:

1. Clicar no menu **Iniciar**
2. Selecionar a opção **Executar**
3. Ao ser perguntado sobre qual programa executar, digitar **`D:\br\firewall\criptoc\instalar`**. (Caso o leitor de CD-ROM seja acessado por uma letra diferente de D, substituí-la pela letra equivalente, no comando anterior).

A janela de instalação será mostrada. Para prosseguir, siga as instruções apresentadas na tela.

Ao término da instalação, será criado um grupo chamado **Firewall Aker**, no menu **Iniciar**. Dentro deste grupo será criado um novo grupo chamado de **Cliente de**

Criptografia. Para se executar o cliente de criptografia, basta selecionar a opção **Cliente de Criptografia**, dentro do grupo com o mesmo nome.

Instalando o cliente através de scripts

Para facilitar a instalação do Cliente de Criptografia Aker em um grande número de máquinas, é possível automatizá-la e realizá-la de forma não interativa. Com isso, pode-se escrever um script de logon, por exemplo, que instale o cliente caso ele já não esteja instalado.

A instalação automática, não interativa, é acionada através de um outro programa, chamado de **`Setupbat`**, localizado no mesmo diretório do programa de instalação descrito acima. Ele recebe as opções de instalação através da linha de comando, sendo que as seguintes opções estão disponíveis:

`-a`	Executa instalação automática
`-i`	Adiciona cliente no menu **Iniciar**
`-d` ***`diretório`***	Especifica diretório de instalação
`-f`	Instala cliente mesmo se já detectar uma instalação anterior
`-c`	Inicia o cliente após instalá-lo

Caso não se tenha especificado a opção **`-d diretório`**, o cliente será instalado em **`C:\Arquivos de Programas\aker\aker_crypt`**

Distribuindo uma configuração padrão na instalação do cliente

Além de instalar o cliente automaticamente, é possível também distribuir uma configuração padrão, que será utilizada tanto na instalação automática quanto na interativa. Desta forma, o administrador de um firewall pode deixar toda a configuração do Cliente de Criptografia Aker pronta, de forma que os usuários finais não necessitem realizar qualquer tipo de configuração.

Para instalar o cliente com uma configuração padrão, basta se configurá-lo em uma máquina, da forma desejada, e a seguir copiar determinados arquivos para o diretório de onde as versões padronizadas serão instaladas. O programa de instalação detectará que os arquivos existem e automaticamente os copiará para o diretório onde o programa será instalado.

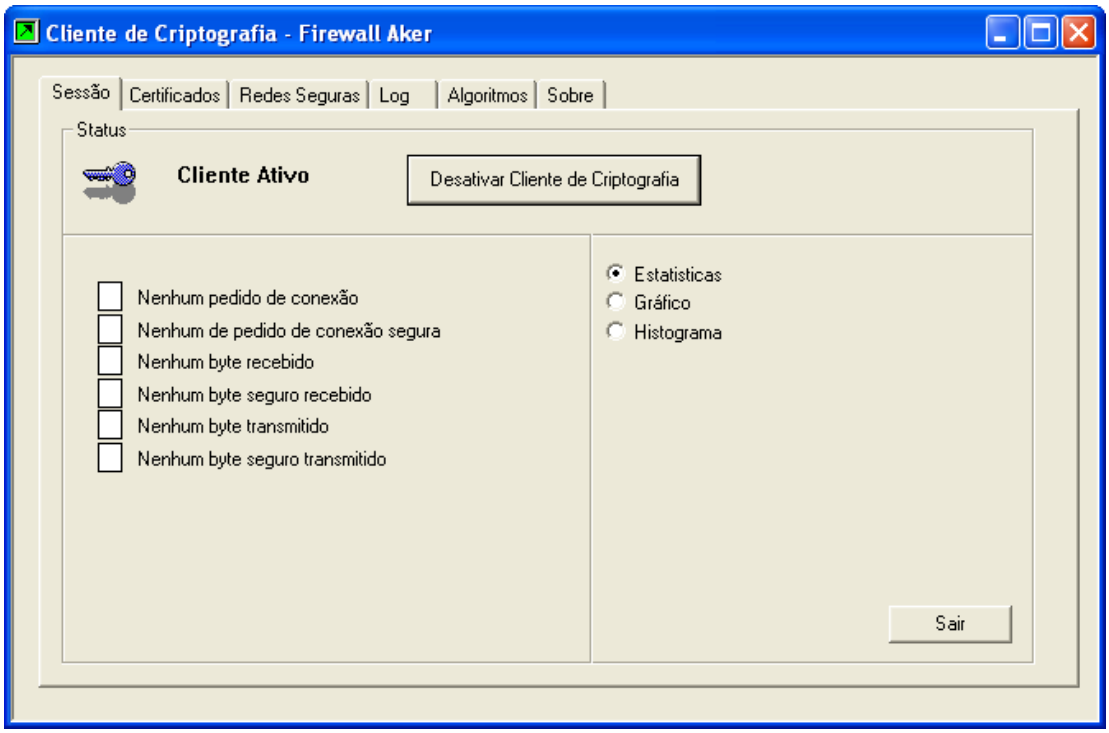
Os seguintes arquivos podem ser copiados:

`nets.cla`	Configuração das redes seguras e opção do uso do Cliente de Autenticação Aker para efetuar logon
`algorithms.cla`	Lista de algoritmos habilitados
`certs.cla`	Certificados de revogação e das entidades certificadoras

9-5 Configurando o Cliente de Criptografia

Quando o Ciente de Criptografia está rodando, um ícone é mostrado na barra de tarefas próximo ao relógio. Para configurá-lo, basta se clicar uma vez sobre este ícone, o que provocará o aparecimento da janela de monitoramento e configuração do cliente. Esta janela consiste de 6 pastas, cada uma responsável por uma parte da configuração:

Sessão

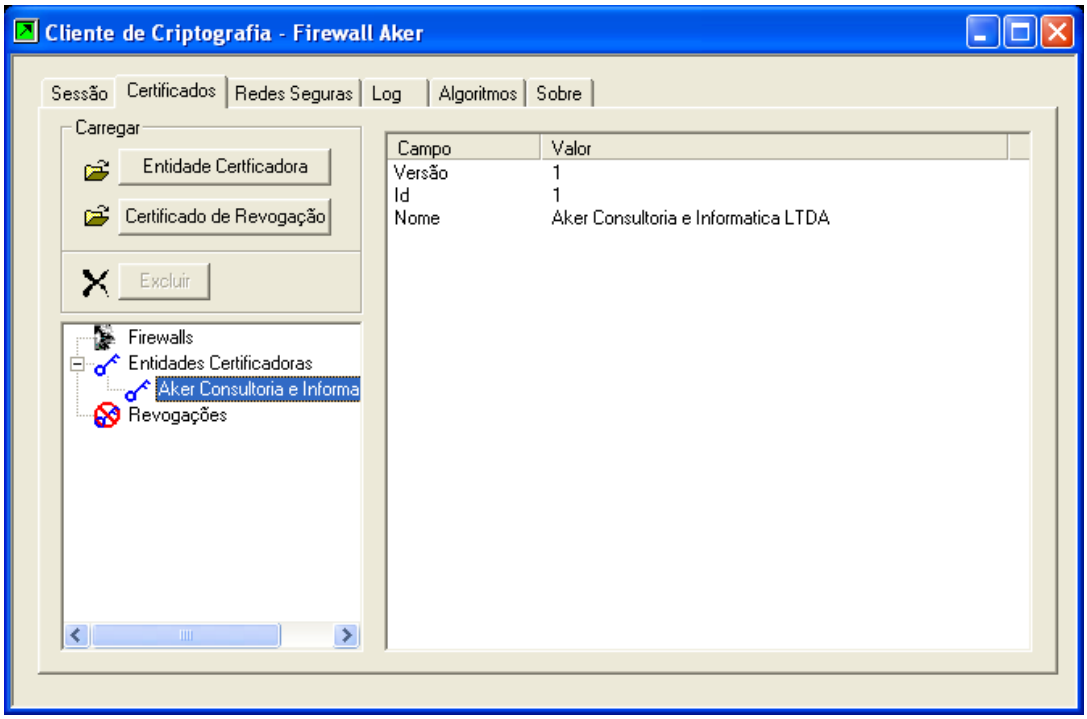


Nesta pasta é mostrado um resumo do funcionamento do Cliente, indicando se o mesmo se encontra ativo ou não e a quantidade de bytes e conexões seguras e não seguras que já passaram pelo Cliente desde o início de seu funcionamento.

Conexões seguras são aquelas que estão sendo encriptadas e as não seguras são aquelas cujos dados trafegam em texto pleno.

Na parte superior da pasta existe um botão que permite que se ative ou desative o Cliente. Caso o Cliente esteja desativado, nenhuma conexão será encriptada.

Certificados



Esta pasta tem o funcionamento igual ao da janela de certificados do firewall, com a única diferença de que não existem certificados locais.

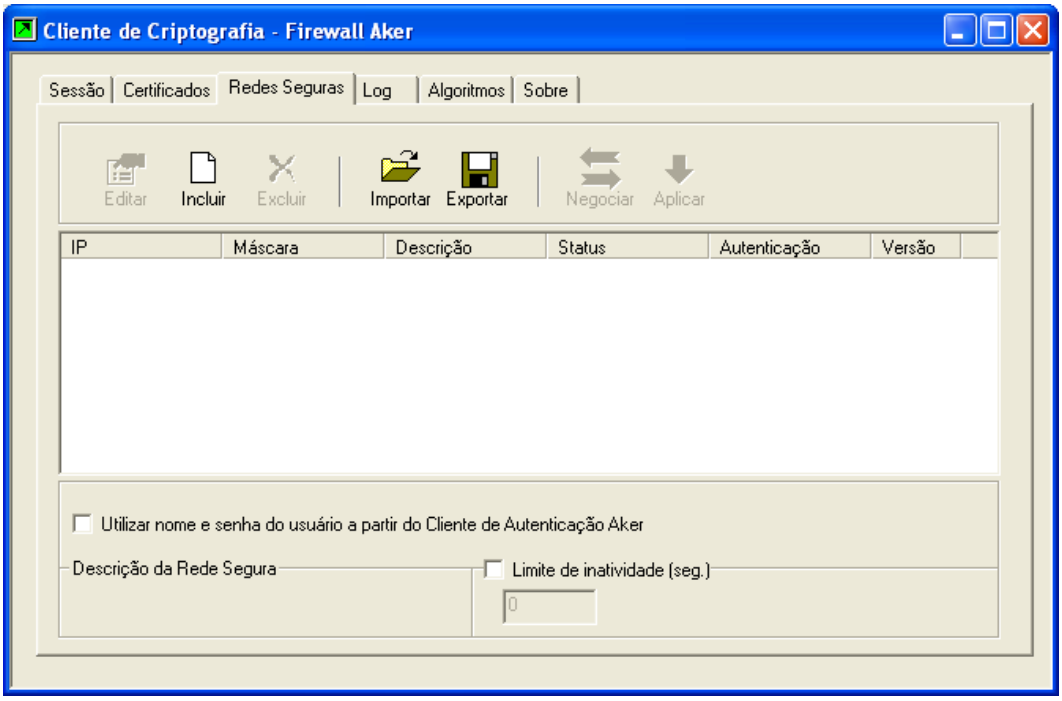
Ela consiste de duas listas: na lista da esquerda são mostrados os certificados de negociação, revogação e de entidades certificadoras. Na lista da direita são mostrados os campos de um certificado que esteja selecionado. Caso nenhum certificado esteja selecionado, ela ficará em branco.

Os campos de cada certificado, mostrados à direita, são apenas informativos. Não é possível se alterar nenhum destes valores.

Para se carregar um novo certificado, deve-se proceder da seguinte forma:

1. Clica-se em um dos botões **Entidade Certificadora** ou **Certificado de Revogação**, no grupo *Carregar*, dependendo do tipo de certificado a ser carregado.
2. Será mostrada uma janela para que se escolha o nome e a localização do arquivo a ser carregado. Após se especificar este nome, deve-se clicar no botão **Abrir**.

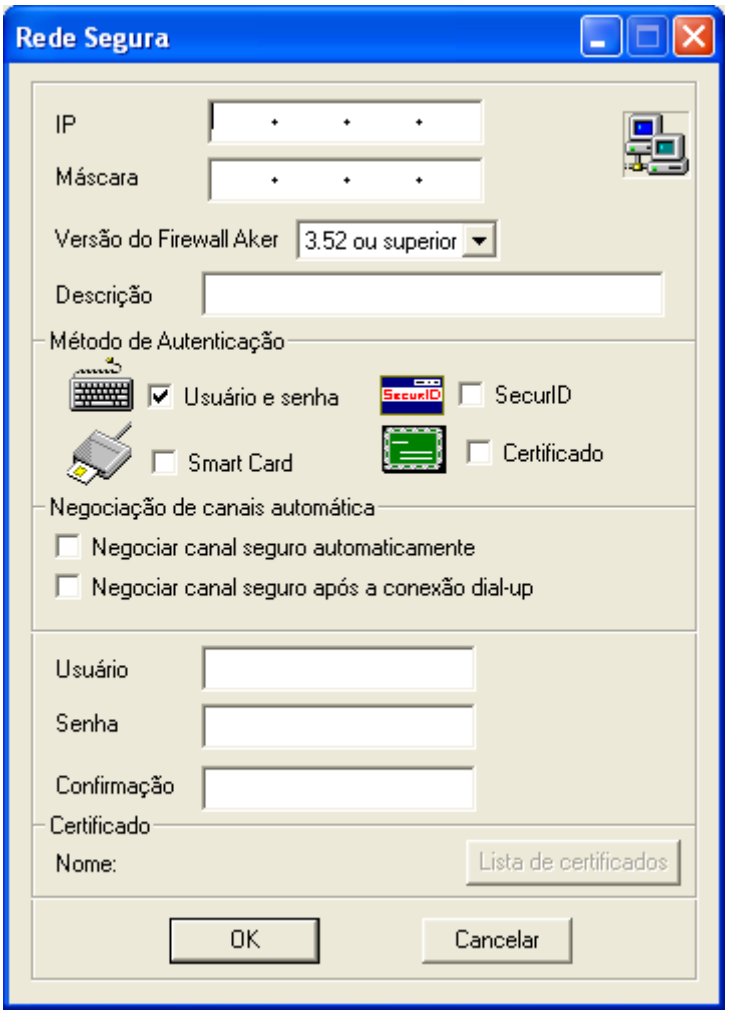
Redes Seguras



Esta é a pasta principal da configuração do Cliente. Ela consiste de uma lista onde são mostradas todas as redes para as quais a comunicação será encriptada. Para cada rede existe uma coluna de status indicando se ela está ativa ou não.

Para se incluir uma nova entrada na lista, basta se clicar no botão **Incluir**, localizado na barra de ferramentas. Para se remover ou editar uma rede segura, basta se selecionar a entrada a ser removida ou editada e clicar na opção correspondente da barra de ferramentas.

No caso das opções *Incluir* ou *Editar* será mostrada seguinte janela:



IP: É o endereço IP da rede com a qual a comunicação será encriptada.

Máscara: É a máscara da rede com a qual a comunicação será encriptada.

Descrição: É um campo livre, utilizado apenas para fins de documentação

É possível se exportar a configuração atual para um arquivo e importá-la posteriormente na mesma ou em outra máquina. Para tal, existem os botões **Importar** e **Exportar**, localizados na barra de ferramentas. O botão **Importar** salva a lista de redes seguras em um arquivo e o botão **Exportar** carrega uma lista de redes a partir de um arquivo e as acrescenta na lista atual (as novas entradas serão acrescentadas ao final da lista atual).

O botão **Negociar** permite que se negocie imediatamente um canal seguro com a rede selecionada. Caso a sessão para a rede selecionada já esteja estabelecida ou nenhuma entrada esteja selecionada, este botão será desabilitado.

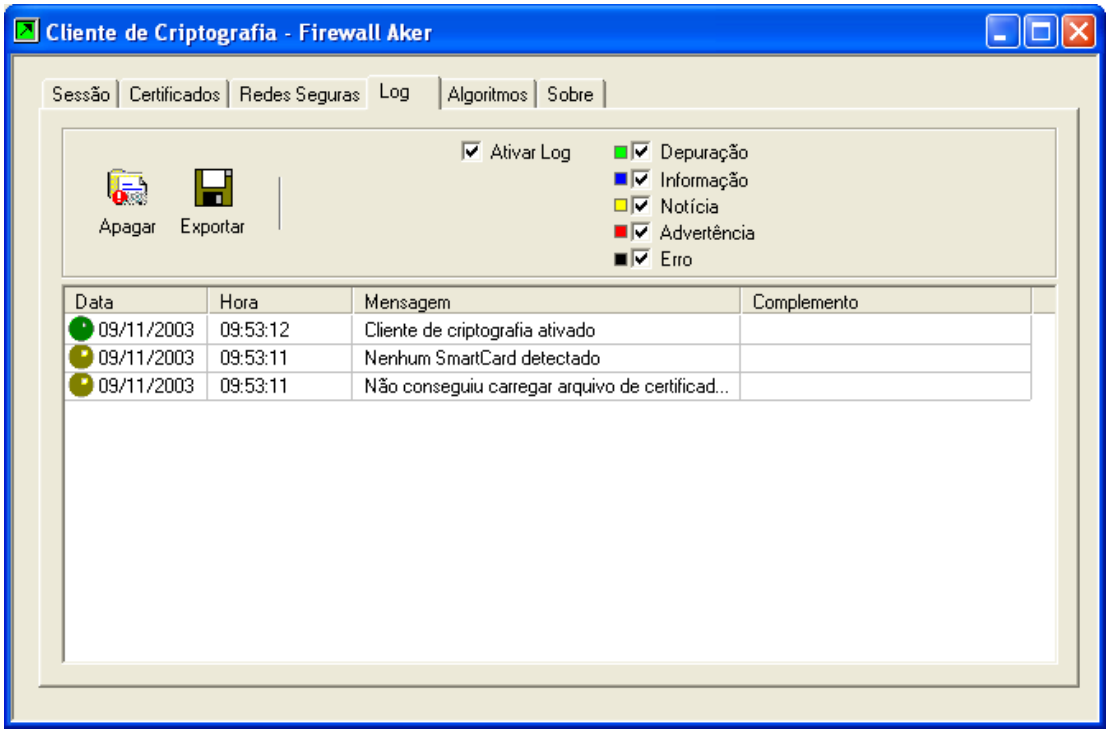
O botão **Aplicar** serve para que as alterações recém feitas sejam salvas se tornem permanentes. Ao ser clicado, todas as sessões que por ventura estejam ativas serão derrubadas.

A opção **Utilizar nome e senha a partir do Cliente de Autenticação Aker**, se estiver marcada, faz com que o cliente de criptografia use a senha e o nome do usuário

utilizados no logon da rede para estabelecer sessões seguras, caso estas exijam autenticação de usuário. Caso esta opção não esteja marcada e o firewall esteja configurado para exigir autenticação de usuários, uma janela pedindo um nome e uma senha será mostrada todas as vezes que uma nova sessão de criptografia for estabelecida.

Caso o Cliente de Autenticação não esteja ativo, a opção **Utilizar nome e senha a partir do Cliente de Autenticação Aker** estará desabilitada, não podendo ser utilizada.

Log



Esta pasta é muito útil para se acompanhar o funcionamento do cliente de criptografia. Ela consiste de uma lista com diversas mensagens ordenadas pela hora. Ao lado de cada mensagem existe um ícone colorido, simbolizando sua prioridade. As cores tem o seguinte significado:

Verde	Depuração
Azul	Informação
Amarelo	Notícia
Vermelho	Advertência
Preto	Erro

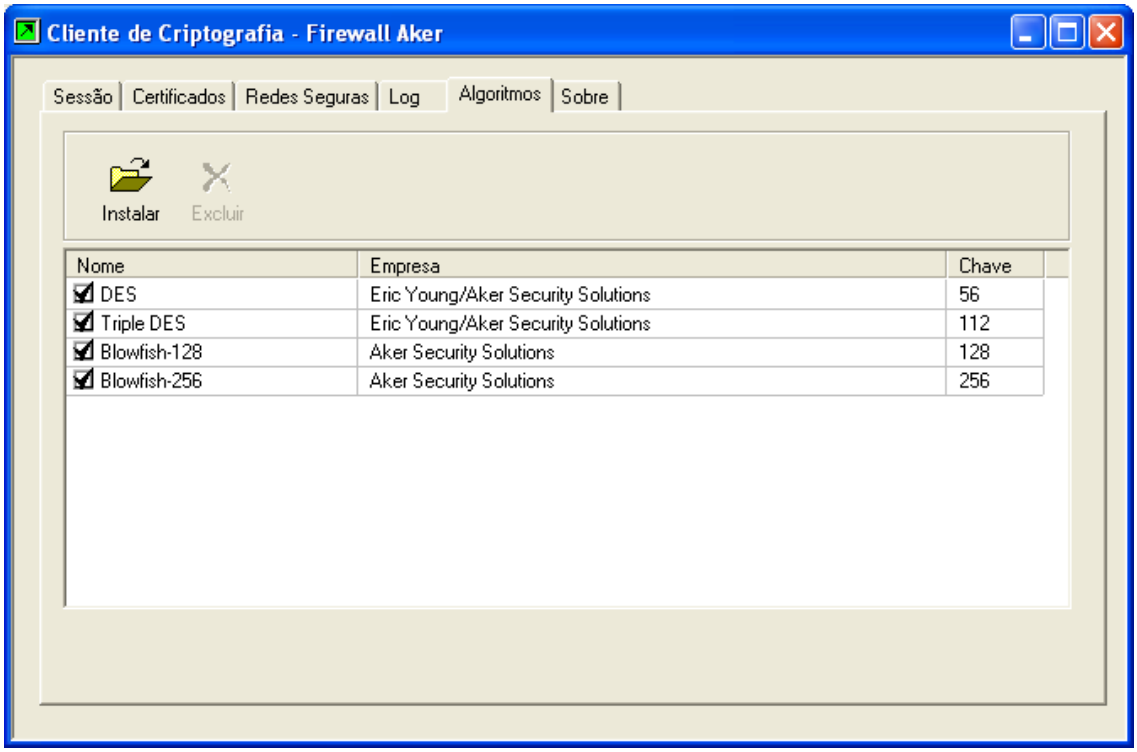
O botão **Apagar**, localizado na barra de ferramentas permite com que se apague todas as entradas existentes no log.

O botão **Salvar**, localizado na barra de ferramentas permite com que se salve o log em um arquivo formato texto. Ao ser clicado, será mostrada uma janela para que se especifique o nome do arquivo que será salvo.

A opção **Ativar Log**, se estiver desmarcada, fará com que novas entradas de log não sejam mais geradas pelo Cliente de Criptografia.

O log do Cliente de Criptografia Aker é armazenado apenas durante a execução do cliente. Caso este seja fechado, todas as suas informações serão descartadas.

Algoritmos



A pasta de algoritmos permite com que se desabilite determinados algoritmos, fazendo com que estes não sejam utilizados no estabelecimento de canais seguros, bem como que se carregue novos algoritmos e se remova algoritmos previamente carregados. Ela consiste de uma lista onde, para cada algoritmo, é mostrado seu nome, empresa ou pessoa que o implementou e o tamanho, em bits, de sua chave.

Para se desabilitar um algoritmo, basta se clicar sobre a caixa à esquerda de seu nome. Um novo clique o habilitará novamente.

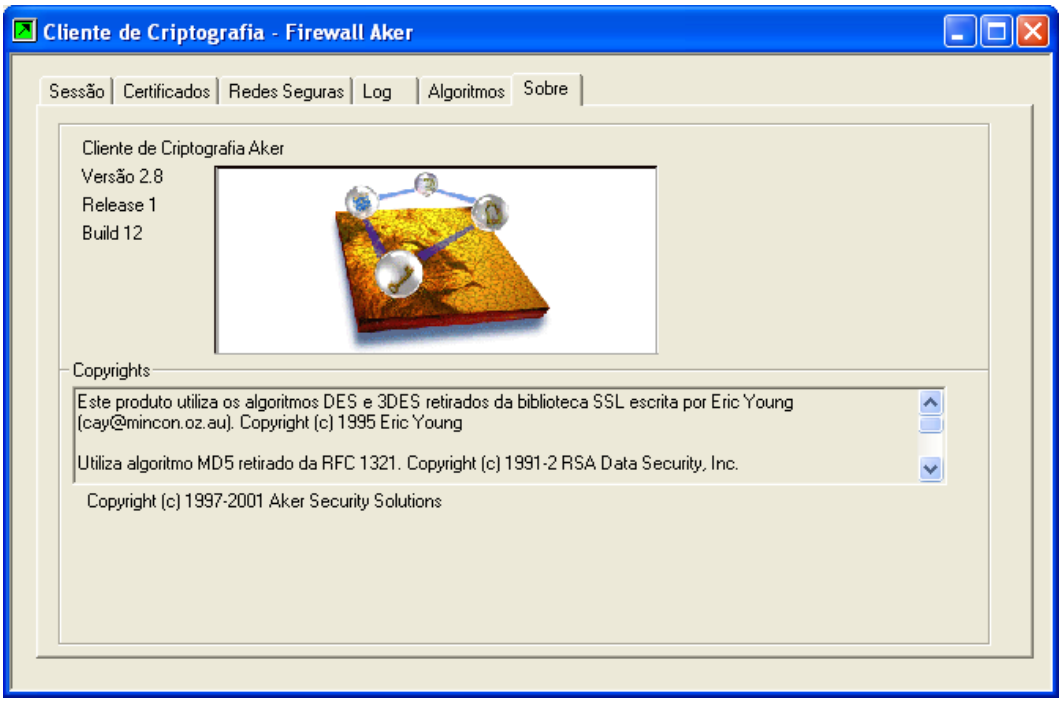
Para se adicionar um novo algoritmo ao Cliente de Criptografia, basta se clicar sobre o botão **Instalar**, localizado na barra de ferramentas. Será mostrada então uma janela para que se possa especificar o nome do arquivo .DLL, fornecido pelo fabricante do algoritmo, que contém sua implementação.

Para se remover um algoritmo, basta clicar sobre seu nome, para selecioná-lo, e então clicar no botão **Excluir**, localizado na barra de ferramentas. Este procedimento removerá o arquivo .DLL instalado por meio da opção anterior.

Para se realizar qualquer operação sobre os algoritmos, é necessário que o Cliente de Criptografia esteja inativo.

Não é possível se excluir os algoritmos padrão do Cliente de Criptografia, sendo apenas possível desabilitá-los.

Sobre


Cliente de Criptografia - Firewall Aker
Sessão
Certificados
Redes Seguras
Log
Algoritmos
Sobre
Cliente de Criptografia Aker
Versão 2.8
Release 1
Build 12
Copyrights
Este produto utiliza os algoritmos DES e 3DES retirados da biblioteca SSL escrita por Eric Young (cay@mincon.oz.au). Copyright (c) 1995 Eric Young
Utiliza algoritmo MD5 retirado da RFC 1321. Copyright (c) 1991-2 RSA Data Security, Inc.
Copyright (c) 1997-2001 Aker Security Solutions

Esta é uma pasta meramente informativa e serve para que se obtenha algumas informações do Cliente de Criptografia. Dentre as informações úteis se encontram sua versão e release.

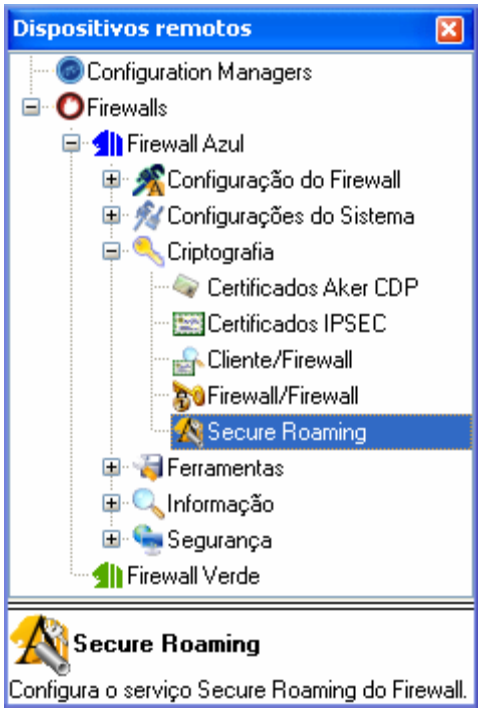
10-0 Configurações do Secure Roaming

Aqui você encontra as instruções necessárias para configurar corretamente o Secure Roaming do firewall.

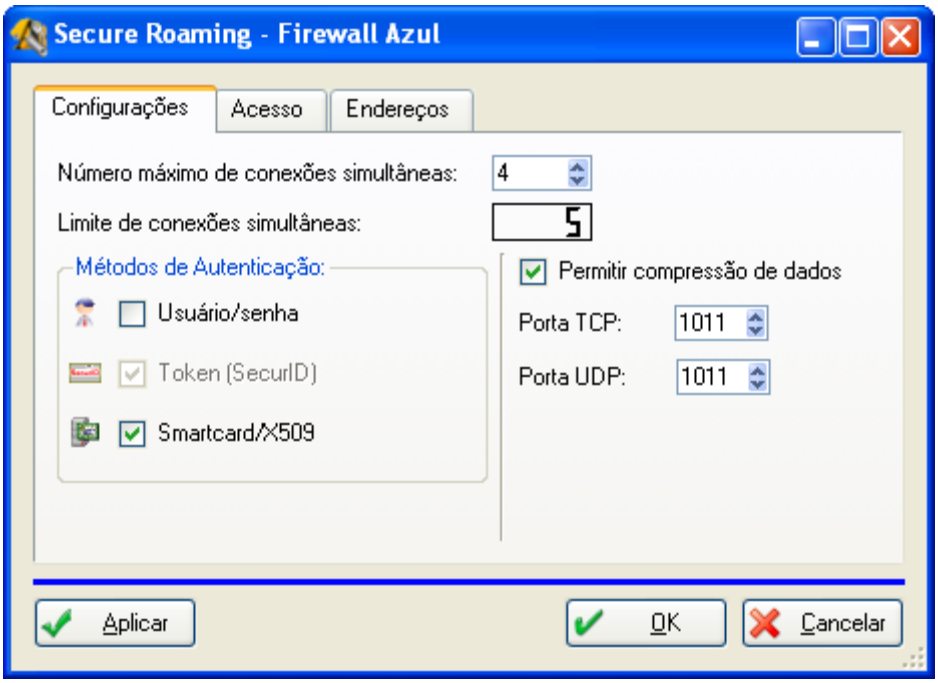
10-1 Utilizando a interface gráfica

Para ter acesso à janela de configurações do Secure Roaming basta:

- Clicar no menu *Criptografia* da janela principal
- Escolher o item *Secure Roaming*



A janela de configurações do Secure Roaming



- O botão **OK** fará com que a janela de configurações do Secure Roaming seja fechada e as alterações efetuadas aplicadas.
- O botão **Cancelar** fará com que a janela seja fechada porém as alterações efetuadas não sejam aplicadas.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

---

Aba Configurações

- **Número máximo de conexões simultâneas**: Aqui você pode configurar o número máximo de clientes conectados simultaneamente no Secure Roaming em um determinado tempo. Use esta opção para evitar com que o servidor tenha uma sobrecarga por excesso de clientes, o que pode diminuir a perfomance. Por favor, note que este número não pode ser superior ao de sua licença. Se estiver em 0, nenhum cliente será permitido.

- **Limite de conexões simultâneas**: Indica o limite máximo de conexões permitido por sua licença.

- **Métodos de Autenticação**: As opções disponíveis, que podem ser marcadas independentemente, são:
    1. **Usuário/senha:** O usuário deverá se autenticar através de uma combinação de nome e uma senha. Esses dados serão repassados a um ou mais servidores de autenticação que deverão validá-los. Esta opção é a mais insegura porém não depende de nenhum hardware adicional.
    2. **Token (SecurID):** O usuário deverá se autenticar mediante o fornecimento de um nome, um PIN e um código presente em um Token SecurID que é modificado a cada minuto. Esses dados serão repassados para o autenticador Token cadastrado no firewall para serem validados.

Essa opção é bem mais segura que a anterior, porém exige que cada usuário possua um Token.

3. **Smartcard/X509:** O usuário deverá se autenticar através do uso de certificados X509 (por exemplo, gravados em smart cards) e emitidos por uma das autoridades certificadoras cadastradas no firewall. Essa forma de autenticação é a mais segura das três, por exigir a senha de desbloqueio da chave privada e a posse da mesma.

- **Permitir compressão de dados**: A compressão de dados é importante para conexões lentas, como as discadas. Quando esta opção está marcada, é feita a compressão das informações antes de serem enviadas pela rede. Isso permite um ganho de performance na velocidade de comunicação, porém, exige um maior processamento local. Para redes mais rápidas, é melhor não se utilizar a compreesão.

- **Porta TCP/UDP**: Este controle permite configurar a porta usada pelo servidor para escutar conexões e dados de clientes, respectivamente. Por exemplo, você pode configurar o servidor para usar as portas TCP/443 e UDP/53, em ordem para burlar firewalls e/ou outros dispositivos de filtragem entre servidores e clientes. Esses dispositivos recusariam uma conexão VPN, mas não uma conexão HTTP segura e uma requisição DNS, respectivamente.
  A porta padrão é **1011** tanto para TCP e UDP .

Aba Acesso

- **Tipo da lista de controle de acesso**: Aqui você escolhe qual é o tipo da *Lista de controle de acesso*:
  1. **Nenhum**: Sem controle de acesso. Todo cliente tem permissão para conectar ao servidor.

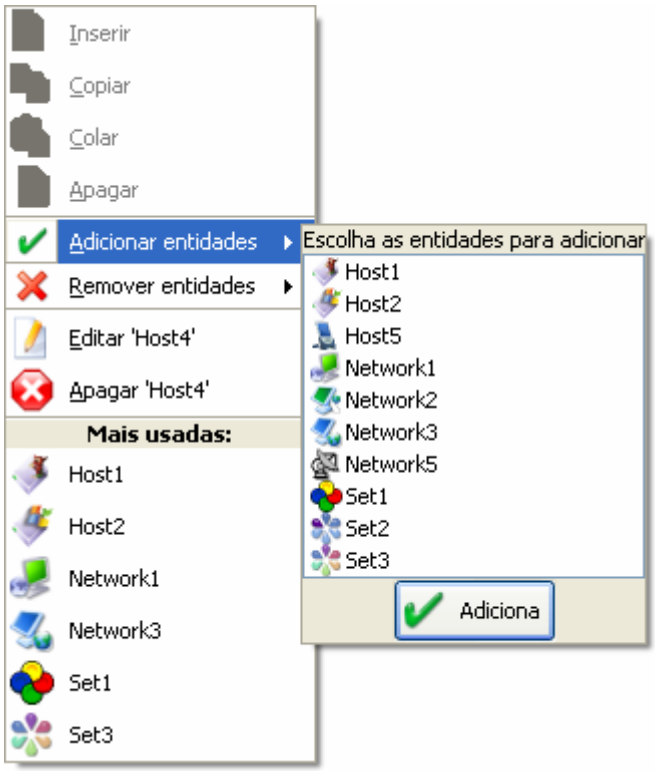
2. **Permitir entidades listadas**: Somente os endereços IP listados, ou endereços que pertençam às entidades rede e/ou conjunto listadas, poderão estabelecer conexão.
3. **Proibir entidades listadas**: As entidades listadas, ou que pertençam a entidades rede e/ou conjunto listadas, não serão capazes de estabelecer conexões. As demais entidades serão.

- **Lista de controle de acesso**:
  Para se adicionar uma entidade à lista, deve-se proceder da seguinte forma:
  - Clique com o botão direito do mouse na lista, ou
  - arraste a entidade do campo entidades, localizado no lado inferior esquerdo, para a lista.

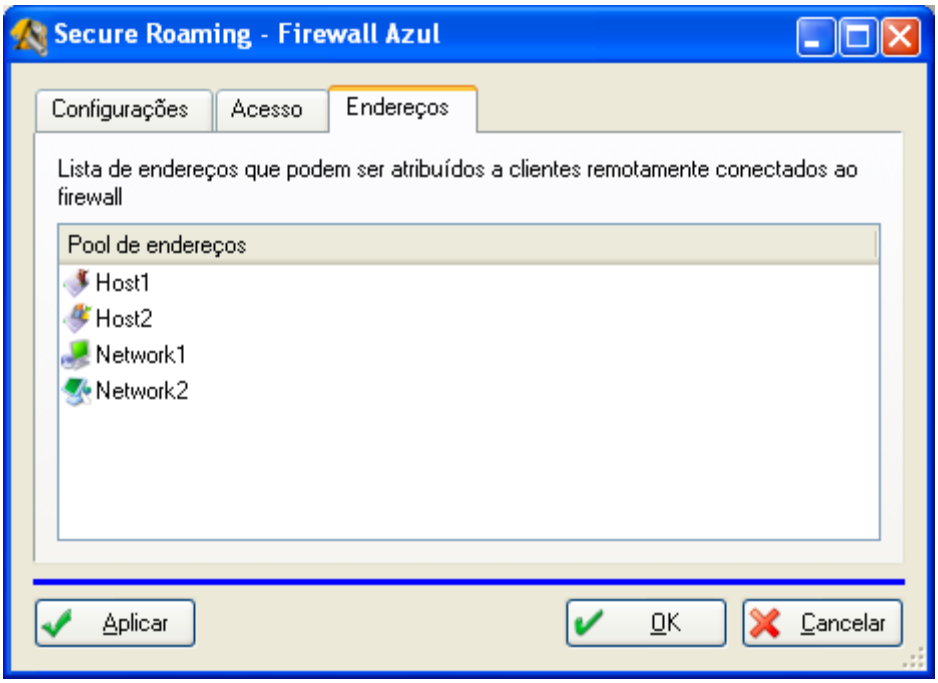
  Para se remover uma entidade, deve-se proceder da seguinte forma:

  - Clica-se com o botão direito do mouse sobre a entidade que será removida, ou
  - selecione a entidade desejada e pressione a tecla *Delete*.

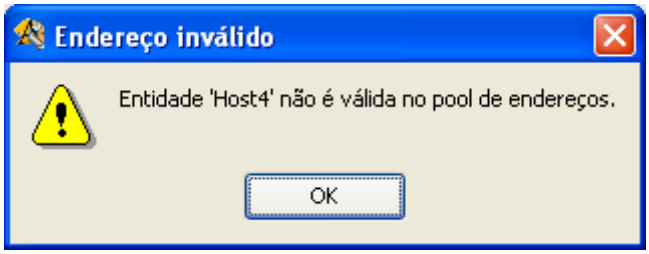
  A figura a seguir mostra o menu popup com todas as opções listadas acima. Ele é mostrado ao se clicar com o botão direito do mouse em alguma entidade listada. No exemplo da figura, a entidade clicada foi *Host4*:



Aba Endereços



- **Pool de endereços**: Lista de endereços que podem ser atribuídos a clientes remotamente conectados ao firewall. Os endereços de máquinas listados e todos os endereços que compõem as redes e conjuntos incluídos somam-se para definir o conjunto de endereços atribuíveis a clientes.
  Notar que as entidades listadas devem estar conectadas a algum adaptador de rede configurado no firewall. Caso contrário, não será possível estabelecer conexão com tal entidade e a seguinte mensagem será mostrada:



Para adicionar ou remover uma entidade do *Pool de endereços*, basta proceder como na *Lista de controle de acesso*.

As redes nesse campo definem um conjunto de endereços, não uma sub-rede no sentido de roteamento IP. Isso quer dizer que, por exemplo, se a interface do firewall estiver na sub-rede 10.0.0.0/255.0.0.0 e a rede 10.0.0.0/255.255.255.0 for incluída no Pool de endereços, o primeiro endereço atribuível seria 10.0.0.1 e o último 10.0.0.255. Se fosse a rede 10.1.0.0/255.255.255.0, a faixa iria de 10.1.0.0 a 10.1.0.255, incluindo-se ambos os extremos.

11-0 Integração dos Módulos do Firewall

Neste capítulo será mostrada a relação entre os três grandes módulos do Firewall Aker: o filtro de pacotes, o conversor de endereços e o módulo de criptografia e autenticação. Será mostrado também o fluxo pelo qual os pacotes atravessam desde sua chegada no Firewall até o momento de serem aceitos ou rejeitados.

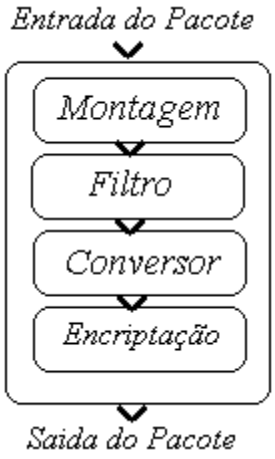
11-1 O fluxo de pacotes no Firewall Aker

Nos capítulos anteriores deste manual foram mostrados separadamente os três grandes módulos do Firewall Aker e todos os detalhes pertinentes à configuração de cada um. Será mostrado agora como um pacote os atravessa e quais alterações ele pode sofrer em cada um deles.

Basicamente, existem dois fluxos distintos: um para pacotes que são emitidos pela rede interna e tem como destino alguma máquina da rede externa (fluxo de dentro para fora) ou pacotes que são gerados na rede externa e tem como destino alguma máquina da rede interna (fluxo de fora para dentro).

O fluxo de dentro para fora

Todo o pacote da rede interna ao atingir o firewall passa pelos módulos na seguinte ordem: módulo de montagem, filtro de pacotes, conversor de endereços e módulo de encriptação.



- **O módulo de montagem**

O módulo de montagem é o responsável por armazenar todos os fragmentos de pacotes IP recebidos até que estes possam ser montados e convertidos em um pacote completo. Este pacote será então entregue para os demais módulos.

- **O filtro de pacotes**

O filtro de pacotes possui a função básica de validar um pacote de acordo com as regras definidas pelo administrador, e a sua tabela de estados, e decidir se este deve ou não ser autorizado a trafegar pelo firewall. Se ele decidir que o pacote pode trafegar, este será repassado para os demais módulos, caso contrário será descartado e o fluxo terminado.

- **O conversor de endereços**

O conversor de endereços recebe um pacote já autorizado a trafegar e verifica, de acordo com sua configuração, se este deve ter o endereço de origem convertido. Em caso positivo, ele o converte, do contrário o pacote não sofre quaisquer alterações.

Independente de ter sido convertido ou não, o pacote será repassado para o módulo de criptografia.

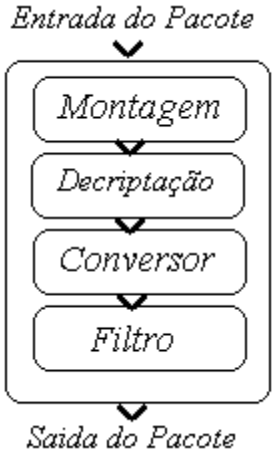
- **O módulo de encriptação**

O módulo de encriptação recebe um pacote validado e com os endereços convertidos e decide, baseado em sua configuração, se este pacote deve ser encriptado ou autenticado antes de ser enviado ao destino. Em caso positivo, o pacote será autenticado, encriptado, e sofrerá o acréscimo de cabeçalhos específicos destas operações.

Independentemente de ter sido encriptado/autenticado ou não, o pacote será enviado pela rede.

O fluxo de fora para dentro

Todo o pacote proveniente da rede externa, em direção à rede interna, ao atingir o firewall passa pelos módulos na seguinte ordem: módulo de montagem, módulo de decriptação, conversor de endereços e filtro de pacotes.



- **O módulo de montagem**

O módulo de montagem é o responsável por armazenar todos os fragmentos de pacotes IP recebidos até que estes possam ser montados e convertidos em um pacote completo. Este pacote será então entregue para os demais módulos.

- **O módulo de decriptação**

O módulo de decriptação tem a função de remover os cabeçalhos adicionados pelo módulo de encriptação, verificar a assinatura de autenticação do pacote e decriptá-lo. Caso a autenticação ou a criptografia apresentem erro, o pacote será descartado.

A outra função deste módulo é assegurar que todos os pacotes que cheguem de uma rede para a qual existe um canal seguro estejam vindo criptografados. Caso um pacote venha de uma rede para a qual existe um canal de criptografia ou autenticação e este pacote não estiver autenticado ou criptografado, ele será descartado.

Caso o pacote tenha sido validado com sucesso, este será repassado para o conversor de endereços.

- **O conversor de endereços**

O conversor de endereços recebe um pacote e verifica se o endereço destino deste pacote é um dos IPs virtuais. Em caso positivo, este endereço é convertido para um endereço real.

Independente de ter sido convertido ou não, o pacote será repassado para o filtro de pacotes.

- **O filtro de pacotes**

O filtro de pacotes é o último módulo do fluxo de fora para dentro. Ele possui a função básica de validar os pacotes recebidos de acordo com as regras definidas pelo administrador, e a sua tabela de estados, e decidir se este deve ou não ser autorizado a trafegar pelo firewall. Se ele decidir que o pacote pode trafegar, este será repassado para a máquina destino, caso contrário ele será descartado.

11-2 Integração do filtro com a conversão de endereços

Quando vai se configurar as regras de filtragem para serem usadas com máquinas cujos endereços serão convertidos surge a seguinte dúvida: deve-se usar os endereços reais das máquinas ou os endereços virtuais ?

Esta dúvida é facilmente respondida ao se analisar o fluxo dos pacotes:

- No fluxo de ida (de dentro para fora), os pacotes passam primeiro pelo filtro e depois possuem seus endereços convertidos (se for o caso), ou seja, o filtro recebe os endereços reais das máquinas.
- No fluxo de volta (de fora para dentro), os pacotes passam primeiro pelo conversor de endereços que converte os endereços destino dos IPs virtuais para os endereços reais. Após isso os pacotes são enviados para o filtro de pacotes, ou seja, novamente o filtro de pacotes recebe os pacotes com os endereços reais.

Em ambos os casos, o filtro não sabe da existência dos endereços virtuais, o que nos leva a fazer a seguinte afirmação:

Ao se criar regras de filtragem deve-se ignorar a conversão de endereços. As regras devem ser configuradas como se as máquinas origem e destino estivessem conversando diretamente entre si, sem o uso de qualquer tipo de conversão de endereços

11-3 Integração do filtro com a conversão e a criptografia

No tópico anterior, mostramos como configurar as regras de filtragem para máquinas cujos endereços serão convertidos. A conclusão foi de que se deveria trabalhar apenas com os endereços reais, ignorando a conversão de endereços. Agora, pode-se acrescentar mais uma pergunta: ao se configurar os fluxos de criptografia para máquinas que sofrerão conversão de endereços, deve-se usar os endereços reais destas máquinas ou os endereços virtuais ?

Para responder esta pergunta, novamente deve-se analisar o fluxo dos pacotes:

- No fluxo de ida (de dentro para fora), os pacotes passam primeiro pelo filtro, depois possuem seus endereços convertidos (se for o caso) e por fim são repassados para o módulo de encriptação. Devido a isso, o módulo de encriptação recebe os pacotes como se eles fossem originados dos endereços virtuais.
- No fluxo de volta (de fora para dentro), os pacotes passam primeiro pelo módulo de decriptação e são decriptados (se for o caso). A seguir são enviados para o conversor de endereços, que converte os IPs virtuais para reais, e por fim são enviados para o filtro de pacotes. O módulo de decriptação recebe os pacotes antes deles terem seu endereço convertido e, portanto, com os endereços virtuais.

Em ambos os casos, o módulo de criptografia recebe os pacotes como se eles tivessem origem ou destino nos IPs virtuais, o que nos leva à seguinte afirmação:

Ao se criar fluxos de criptografia, deve-se prestar atenção à conversão de endereços. Os endereços de origem e destino devem ser colocados como se o fluxo se originasse ou tivesse como destino IPs virtuais.

12-0 Configurando a Segurança

Mostraremos aqui como configurar a proteção contra ataques no módulo de segurança do Firewall Aker.

12-1 Proteção contra SYN Flood

O que é um ataque de SYN flood ?

SYN Flood é um dos mais populares ataques de negação de serviço (*denial of service*). Esses ataques visam impedir o funcionamento de uma máquina ou de um serviço específico. No caso do SYN Flood, consegue-se inutilizar quaisquer serviços baseados no protocolo TCP.

Para se entender este ataque, é necessário primeiro se entender o funcionamento do protocolo TCP, no que diz respeito ao estabelecimento de conexões:

O protocolo TCP utiliza um esquema de 3 pacotes para estabelecer uma conexão:

1. A máquina cliente envia um pacote para a máquina servidora com um flag especial, chamado de flag de SYN. Este flag indica que a máquina cliente deseja estabelecer uma conexão.
2. A máquina servidora responde com um pacote contendo os flags de SYN e ACK. Isto significa que ela aceitou o pedido de conexão e está aguardando uma confirmação da máquina cliente para marcar a conexão como estabelecida.
3. A máquina cliente, ao receber o pacote com SYN e ACK, responde com um pacote contendo apenas o flag de ACK. Isto indica para a máquina servidora que a conexão foi estabelecida com sucesso.

Todos os pedidos de abertura de conexões recebidas por um servidor ficam armazenados em uma fila especial, que tem um tamanho pré-determinado e dependente do sistema operacional, até que o servidor receba a comunicação da máquina cliente de que a conexão está estabelecida. Caso o servidor receba um pacote de pedido de conexão e a fila de conexões em andamento estiver cheia, este pacote é descartado.

O ataque consiste basicamente em se enviar um grande número de pacotes de abertura de conexão, com um endereço de origem forjado, para um determinado servidor. Este endereço de origem é forjado para o de uma máquina inexistente (muitas vezes se usa um dos endereços reservados descritos no capítulo sobre conversão de endereços). O servidor, ao receber estes pacotes, coloca uma entrada na fila de conexões em andamento, envia um pacote de resposta e fica aguardando uma confirmação da máquina cliente. Como o endereço de origem dos pacotes é falso, esta confirmação nunca chega ao servidor.

O que acontece é que em um determinado momento, a fila de conexões em andamento do servidor fica lotada. A partir daí, todos os pedidos de abertura de conexão são descartados e o serviço inutilizado. Esta inutilização persiste durante alguns segundos,

pois o servidor ao descobrir que a confirmação está demorando demais, remove a conexão em andamento da lista. Entretanto, se o atacante persistir em mandar pacotes seguidamente, o serviço ficará inutilizado enquanto ele assim o fizer.

Nem todas as máquinas são passíveis de serem atingidas por ataques de SYN Flood. Implementações mais modernas do protocolo TCP possuem mecanismos próprios para inutilizarem ataques deste tipo.

Como funciona a proteção contra SYN flood do Firewall Aker ?

O Firewall Aker possui um mecanismo que visa impedir que um ataque de SYN flood seja bem sucedido. Seu funcionamento se baseia nos seguintes passos:

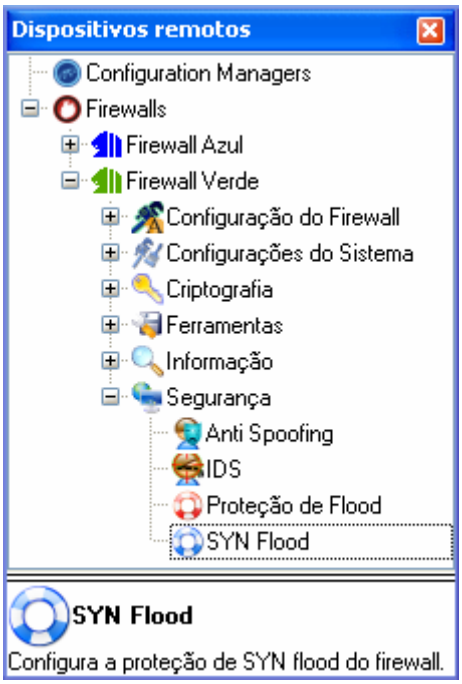
1. Ao chegar um pacote de abertura de conexão (pacote com flag de SYN, mostrado no tópico acima) para uma máquina servidora a ser protegida, o firewall registra isso em uma tabela e deixa o pacote passar (evidentemente, ele só deixará o pacote passar se este comportamento for autorizado pelas regras de filtragem configuradas pelo administrador. Para maiores detalhes veja o capítulo intitulado O filtro de estados).
2. Quando chegar a resposta do servidor dizendo que a conexão foi aceita (pacote com os flags SYN e ACK), o firewall imediatamente enviará um pacote para o servidor em questão confirmando a conexão e deixará o pacote de resposta passar em direção à máquina cliente. A partir deste momento, será acionado um relógio interno no firewall que marcará o intervalo de tempo máximo em que o pacote de confirmação do cliente deverá chegar.
3. Se a abertura de conexão for uma abertura normal, dentro de um intervalo de tempo menor que o máximo permitido, a máquina cliente responderá com um pacote confirmando o estabelecimento da conexão. Este pacote fará o firewall considerar válido o pedido de abertura de conexão e desligar o relógio interno.
4. Caso a máquina cliente não responda dentro do tempo máximo permitido, o firewall mandará um pacote especial para a máquina servidora que fará com que a conexão seja derrubada.

Com estes procedimentos, o firewall consegue impedir que a fila de conexões em andamento na máquina servidora fique cheia, já que todas as conexões pendentes serão estabelecidas tão logo os pacotes de reposta atinjam o firewall. O ataque de SYN flood, portando, não será efetivado.

Cabe enfatizar que todo o funcionamento desta proteção se baseia no intervalo de tempo máximo de espera pelos pacotes de confirmação dos clientes. Se o intervalo de tempo for muito pequeno, conexões válidas podem ser recusadas. Se o intervalo for muito grande, a máquina servidora, no caso de um ataque, ficará com um grande número de conexões abertas o que poderá provocar problemas ainda maiores.

12-2 Utilizando a interface gráfica para Proteção contra SYN Flood

Para ter acesso a janela de configuração dos parâmetros de proteção contra SYN Flood, basta:



- Clicar no menu *Segurança* na janela do Firewall que se deseja administrar
- Escolher o item *SYN Flood*

A janela de configuração da proteção contra SYN flood

- O botão **OK** fará com que os parâmetros de configuração sejam atualizados e a janela fechada.
- O Botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela fechada.

- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

Significado dos campos da janela:
Ativar proteção contra SYN flood: Esta opção deve estar marcada para ativar a proteção contra SYN flood e desmarcada para desativá-la. (ao se desabilitar a proteção contra SYN flood, as configurações antigas continuam armazenadas, mas não podem ser alteradas)

Duração máxima do handshake do TCP: Esta opção define o tempo máximo, em unidades de 500 ms, que o firewall espera por uma confirmação do fechamento das conexões por parte do cliente. Se este intervalo de tempo for atingido, será enviado uma pacote para as máquinas servidoras derrubando a conexão.

O valor ideal deste campo pode variar para cada instalação, mas sugere-se valores entre 3 e 10, que correspondem a intervalos de tempo entre 1,5 e 5 segundos.
A lista de entidades a proteger
A lista de entidades a proteger define as máquinas, redes ou conjuntos que serão protegidos pelo firewall.

Para se incluir uma nova entidade na lista de proteção, deve-se proceder de um dos seguintes modos:

- Executa-se uma operação de *drag-n-drop* (arrastar e soltar) da janela de entidades diretamente para a *lista de hosts e redes a proteger*
- Abre-se o menu de contexto na janela na *lista de hosts e redes a proteger* com o botão direito do mouse ou com a tecla correspondente no.teclado e seleciona-se *Adicionar entidades*, para então escolher aquelas que serão efetivamente incluidas na lista.

Para se remover uma entidade da lista de proteção, deve-se marcá-la e pressionar a tecla *delete*, ou escolher a opção correspondente no menu de contexto, acionado com o botão direito do mouse ou com a tecla correspondente:

Deve-se colocar na lista de entidades a serem protegidas todas as máquinas servidoras de algum serviço TCP passível de ser utilizado por máquinas externas. Não se deve colocar o endereço do próprio firewall nesta lista, uma vez que os sistemas operacionais FreeBSD e Linux não são susceptíveis a ataques de SYN flood.

12-3 Proteção de Flood

O que é um ataque de Flood ?

Os ataques de Flood se caracterizam por existir um elevado número de conexões abertas e estabelecidas contra servidores web, ftp, smtp e etc, a partir de outras máquinas existentes na Internet que foram invadidas e controladas para perpetrar ataques de negação de serviço (DoS).

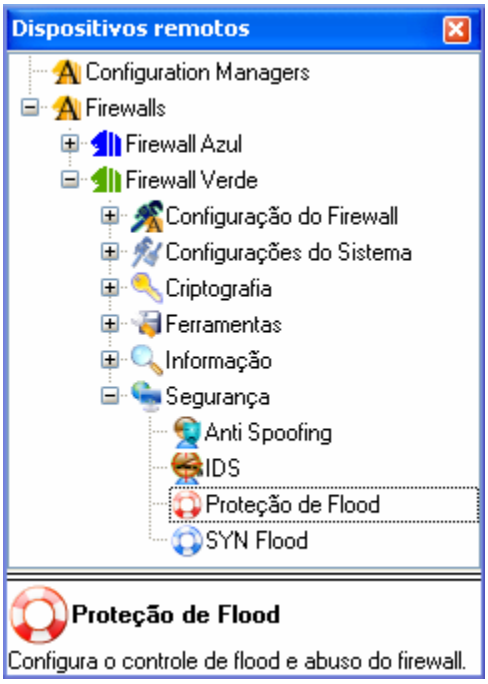
A proteção também é útil para evitar abuso do uso de determinados serviços (sites de download, por exemplo) e evitar estragos maiores causados por vírus, como o NIMDA, que fazia com que cada máquina infectada abrisse centenas de conexões simultaneamente.

Como funciona a proteção contra Flood do Firewall Aker ?

O Firewall Aker possui um mecanismo que visa impedir que um ataque de Flood seja bem sucedido. Seu funcionamento se baseia na limitação de conexões que possam ser abertas simultaneamente a partir de uma mesma máquina para uma entidade que está sendo protegida.

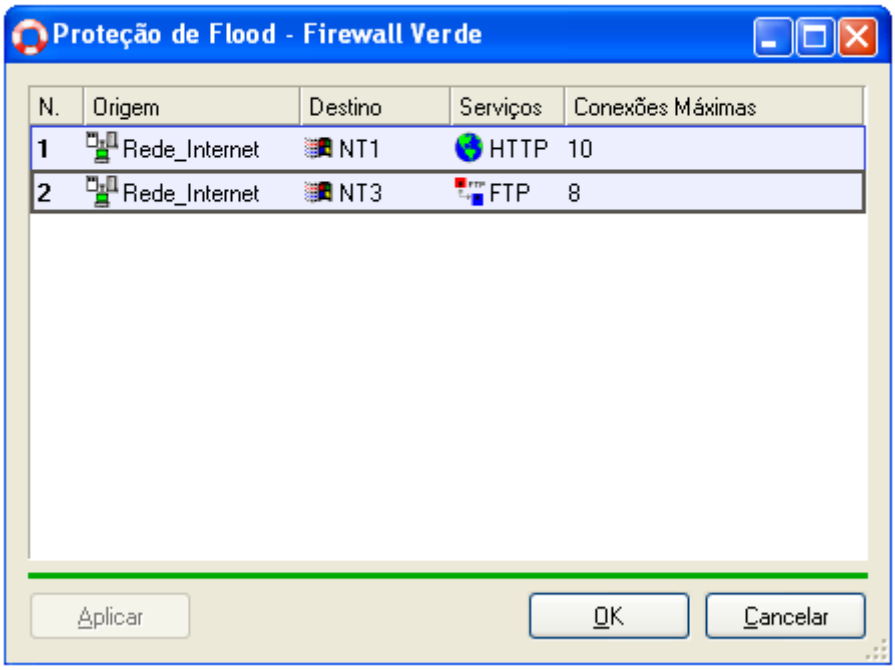
O administrador do firewall deve estimar este limite dentro do funcionamento cotidiano de cada servidor ou rede a ser protegida.

12-4 Utilizando a interface gráfica para Proteção de Flood



- Clicar no menu *Segurança* na janela do Firewall
- Escolher o item *Proteção de Flood*

A janela de configuração da proteção de Flood



- O botão **OK** fará com que os parâmetros de configuração sejam atualizados e a janela fechada.
- O Botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela fechada.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

Significado dos campos da janela:
Número: Corresponde ao número da regra de Proteção de Flood.

Origem: Neste campo pode ser uma rede ou máquina de onde poderá ser originado um ataque de DDoS.

Destino: Incluir neste campo máquinas ou redes que se deseja proteger.

Serviços: portas de serviços que se desejam proteger. Poderá ser incluído no campo mais de uma entidade.

Conexões Máximas: Campo numérico onde se deve informar o número máximo de conexões que a entidade pode receber a partir de uma mesma origem.
A quantidade máxima de conexões nas regras de proteção de flood não é a quantidade agregada de conexões a partir da origem especificada, mas sim a quantidade, por endereço IP único que se encaixe na origem informada, de conexões simultâneas. Desta forma, por exemplo, havendo a necessidade de limitar o número de downloads simultâneos por usuário em 2, esse número dever ser 2, idependentemente do número de usuários que façam os dowloads.

12-5 Proteção Anti Spoofing

O que é um Spoofing ?

O spoofing do IP envolve o fornecimento de informações falsas sobre uma pessoa ou sobre a identidade de um host para obter acesso não-autorizado a sistemas e/ou aos sistemas que eles fornecem. O spoofing interfere na forma como um cliente e um servidor estabelecem uma conexão. Apesar de o spoofing poder ocorrer com diversos protocolos específicos, o spoofing do IP é o mais conhecido dentre todos os ataques de spoofing.

A primeira etapa de um ataque de spoofing é identificar duas máquinas de destino, que chamaremos de A e B. Na maioria dos casos, uma máquina terá um relacionamento confiável com a outra. É esse relacionamento que o ataque de spoofing tentará explorar. Uma vez que os sistemas de destino tenham sido identificados, o violador tentará estabelecer uma conexão com a máquina B de forma que B acredite que tem uma conexão com A, quando na realidade a conexão é com a máquina do violador, que chamaremos de X. Isso é feito através da criação de uma mensagem falsa (uma mensagem criada na máquina X, mas que contém o endereço de origem de A) solicitando uma conexão com B. Mediante o recebimento dessa mensagem, B responderá com uma mensagem semelhante que reconhece a solicitação e estabelece números de sequência.

Sob circunstâncias normais, essa mensagem de B seria combinada a uma terceira mensagem reconhecendo o número de sequência de B. Com isso, o "handshake" seria concluído, e a conexão poderia prosseguir. No entanto, como acredita que está se comunicando com A, B envia sua resposta a A, e não para X. Com isso, X terá de responder a B sem conhecer os números de sequência gerados por B. Portanto, X deverá adivinhar com precisão números de sequência que B utilizará. Em determinadas situações, isso é mais fácil do que possa se imaginar.

No entanto, além de adivinhar o número de sequência, o violador deverá impedir que a mensagem de B chegue até A. Se a mensagem tivesse de chegar a A, A negaria ter solicitado uma conexão, e o ataque de spoofing falharia. Para alcançar esse objetivo, normalmente o intruso enviaria diversos pacotes a máquina A para esgotar sua capacidade e impedir que ela respondesse à mensagem de B. Essa técnica é conhecida como "violação de portas". Uma vez que essa operação tenha chegado ao fim, o violador poderá concluir a falsa conexão.

O spoofing do IP, como acabamos de descrever, é uma estratégia desajeitada e entediante. No entanto, uma análise recente revelou a existência de ferramentas capazes de executar um ataque de spoofing em menos de 20 segundos. O spoofing de IP é uma ameaça perigosa, cada vez maior, mas, por sorte, é relativamente fácil criar mecanismos de proteção contra ela. A melhor defesa contra o spoofing é configurar roteadores de modo a rejeitar qualquer pacote recebido cuja origem alegada seja um host da rede interna. Essa simples precaução impedirá que qualquer máquina externa tire vantagem de relacionamentos confiáveis dentro da rede interna.

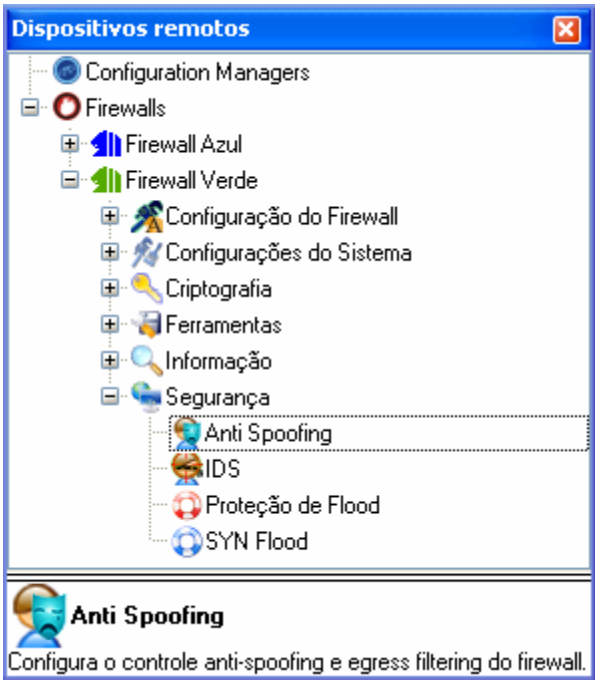
Como funciona a proteção contra Spoofing do Firewall Aker ?

O Firewall Aker possui um mecanismo que visa impedir que um ataque de Spoofing seja bem sucedido. Seu funcionamento se baseia no cadastramento das redes que estão sendo protegidas pelo firewall ou seja, atrás de cada interface de rede do firewall.

Nas redes internas, só serão aceitos pacotes das entidades cadastradas e, das externas, somente pacotes cujo IP origem não se encaixe em nenhuma entidade cadastrada nas redes internas (todas).

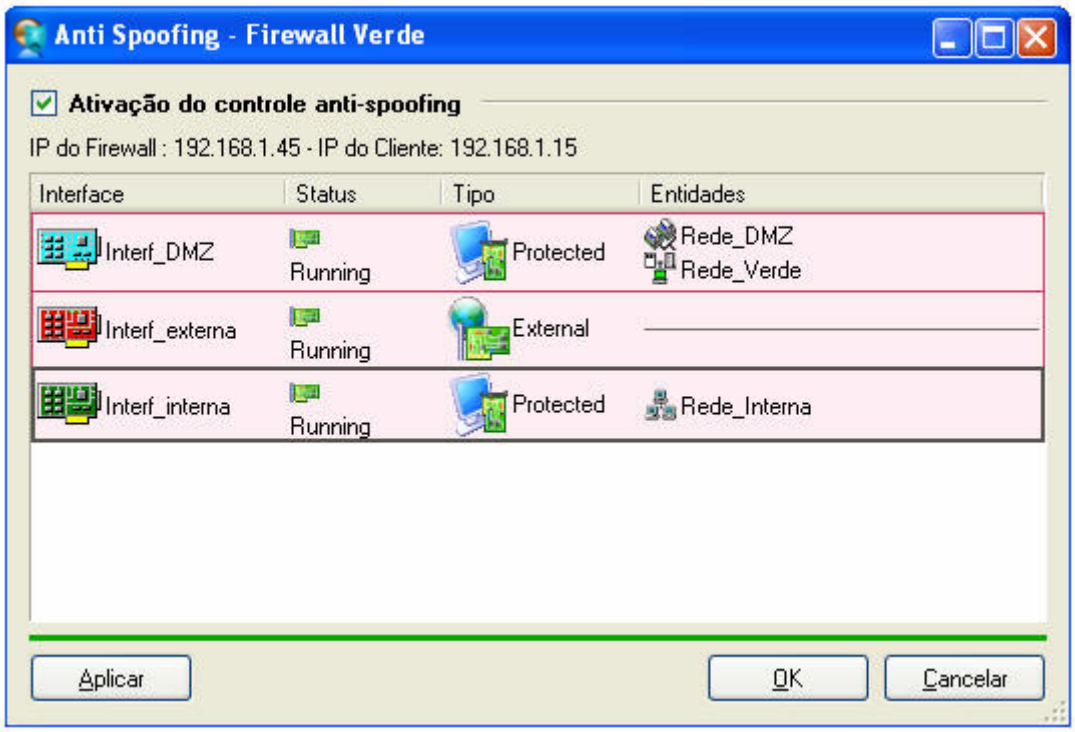
O administrador do firewall deve então fazer o levantamento destas redes, criar as entidades correspondentes e utilizar a interface gráfica para montar a proteção.

12-6 Utilizando a interface gráfica para Anti Spoofing



- Clicar no menu *Segurança* na janela do Firewall
- Escolher o item *Anti Spoofing*

A janela de configuração de Anti Spoofing



- O botão **OK** fará com que os parâmetros de configuração sejam atualizados e a janela fechada.
- O Botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela fechada.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

Significado dos campos da janela:
Ativação do controle anti-spoofing: A marcação da caixa ativa a proteção Anti Spoofing.
Interface: Corresponde a interface cadastrada no firewall pelo administrador.

Status: Neste campo é mostrado o estado da interface, ou seja, se está ativa ou não. Este campo não pode ser editado.

Tipo: Por padrão este campo é marcado como *Externa*. Clicando-se com o botão direito do mouse poderá ser trocado o tipo para *Protegida*, passando o campo *Entidades* para a condição de editável.

Protegida significa que a interface está conectada a uma rede interna e somente serão aceitos pacotes com endereços IP originados em alguma das entidades especificadas na regra. *Externa* significa que é uma interface conectada a Internet da qual serão aceitos pacotes provenientes de quaisquer endereços origem, exceto os pertencentes a entidades listadas nas regras de interfaces marcadas como *Protegidas*.

Entidades: Quanto se define uma interface *Protegida*, deve-se incluir neste campo a lista de todas as redes e/ou máquinas que se encontram conectadas a esta interface.

12-7 Sistema de Detecção de Intrusão (IDS)

O que é um sistema de detecção de intrusão (IDS) ?

Os sistemas de detecção de intrusão têm a habilidade de identificar uma tentativa de acesso à um sistema ou rede que não esteja de acordo com a política de segurança existente na organização. Esta identificação é calculada utilizando-se reconhecimento de padrões de comportamento e dados que são identificados em pacotes ou informações de sistema, que podem corresponder à ataques ou tentativas de invasão a uma rede.

As ferramentas de IDS são soluções de software ou hardware dedicadas à tarefa de identificar e responder automaticamente a atividades que sejam consideradas suspeitas (normalmente são padrões conhecidos de ataques ou ações previamente definidas e configuradas como não autorizadas). As ferramentas IDS reconhecem atividades que não estejam dentro dos seus parâmetros como normais e podem ser programadas para então reconfigurar o firewall dinamicamente (bloqueando possíveis ataques em tempo real), enviar alertas para o administrador, gravar um arquivo de log e até mesmo terminar a conexão.

Como funciona o suporte a agentes IDS no Firewall Aker ?

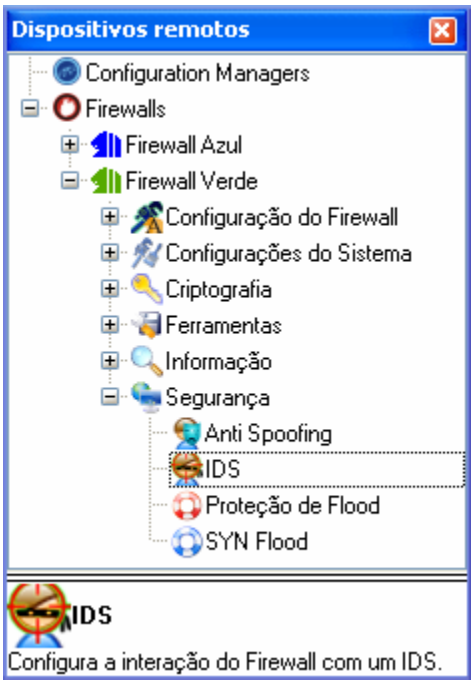
O agente de detecção de intrusão atua direta e dinamicamente no Firewall Aker adicionando regras de bloqueio quando algum dos parâmetros definidos como normais não estejam sendo cumpridos. Por exemplo, suponhamos que o agente monitorando um servidor web esteja configurado para não permitir um número maior que 20 conexões de uma mesma máquina da Internet. Caso este padrão for violado, o agente cadastra dinamicamente uma regra no firewall bloqueando o acesso da máquina de onde estão sendo originadas as conexões. Esta regra pode ser válida por um período de tempo, após o qual ela é automaticamente eliminada, ou indefinidamente, sendo eliminada apenas quando da reinicialização do firewall.

O Firewall Aker possui um *plugin* específico para os produtos Real Secure™, NFR™, Dragon™ e Snort possibilitando sua integração imediata e transparente para o administrador. Neste caso, o administrador deve instalar o *plugin* na máquina onde o agente IDS está instalado e logo após configurá-lo para acrescentar regras de bloqueio no firewall. No firewall, deve-se configurar o suporte para agentes IDS, como explicado no tópico a seguir. É possível a utilização de outros agentes IDS, porém sua integração deve ser feita mediante a criação de scripts. Neste caso, deve-se verificar o tópico que descreve a interface texto, logo abaixo.

As regras de bloqueio do IDS somente serão removidas após expirar seu tempo de duração, por ação do administrador ou reinicialização do Firewall Aker. Nos últimos dois casos, todas as regras temporárias serão removidas (ou seja, não é possível eliminar uma regra específica após esta ter sido acrescentada).

12-8 Configurando o suporte para o agente de detecção de intrusão

Para ter acesso à janela de Detecção de Intrusão basta:



- Clicar no menu *Segurança* da janela principal
- Selecionar o item *IDS*

A janela de detecção de intrusão

Nessa janela são configurados todos os parâmetros que propiciam que agentes IDS acrescentem regras de bloqueio no firewall.

- O botão **OK** fará com que a janela de configuração de agente IDS seja fechada e as alterações efetuadas salvas.
- O botão **Cancelar** fará com que a janela seja fechada porém as alterações efetuadas não sejam aplicadas.

- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

Significado dos parâmetros
Habilitar agente de IDS: Esta opção deve estar marcada para ativar o suporte a agentes IDS e desmarcada para desativá-lo. (ao se desabilitar o suporte a agentes IDS, as configurações antigas continuam armazenadas, mas não podem ser alteradas)

Agente IDS a utilizar: Esse campo indica o agente IDS que estará habilitado a incluir regras de bloqueio no firewall. Esse agente deve ter sido previamente cadastrado no firewall. Para maiores informações veja o capítulo intitulado Cadastrando entidades.

O **Status** permite ao administrador verificar o status da conexão com o agente IDS. Um valor verde, com a palavra *Conectado*, indica que o firewall conseguiu se autenticar e estabelecer com sucesso a comunicação com o agente.

O botão **Atualizar** fará com que o status da conexão seja renovado.

O botão **Descarregar** fará com que todas as regras cadastradas pelo agente IDS sejam excluídas do firewall.

12-9 Instalando o Plugin para agentes IDS no Windows NT

A instalação do plugin para IDS é bastante simples. Para instalá-lo, é necessário colocar o CD-ROM do Firewall Aker na máquina destino ou copiar o conteúdo do diretório de instalação do agente do CD-ROM para algum diretório temporário nesta máquina.

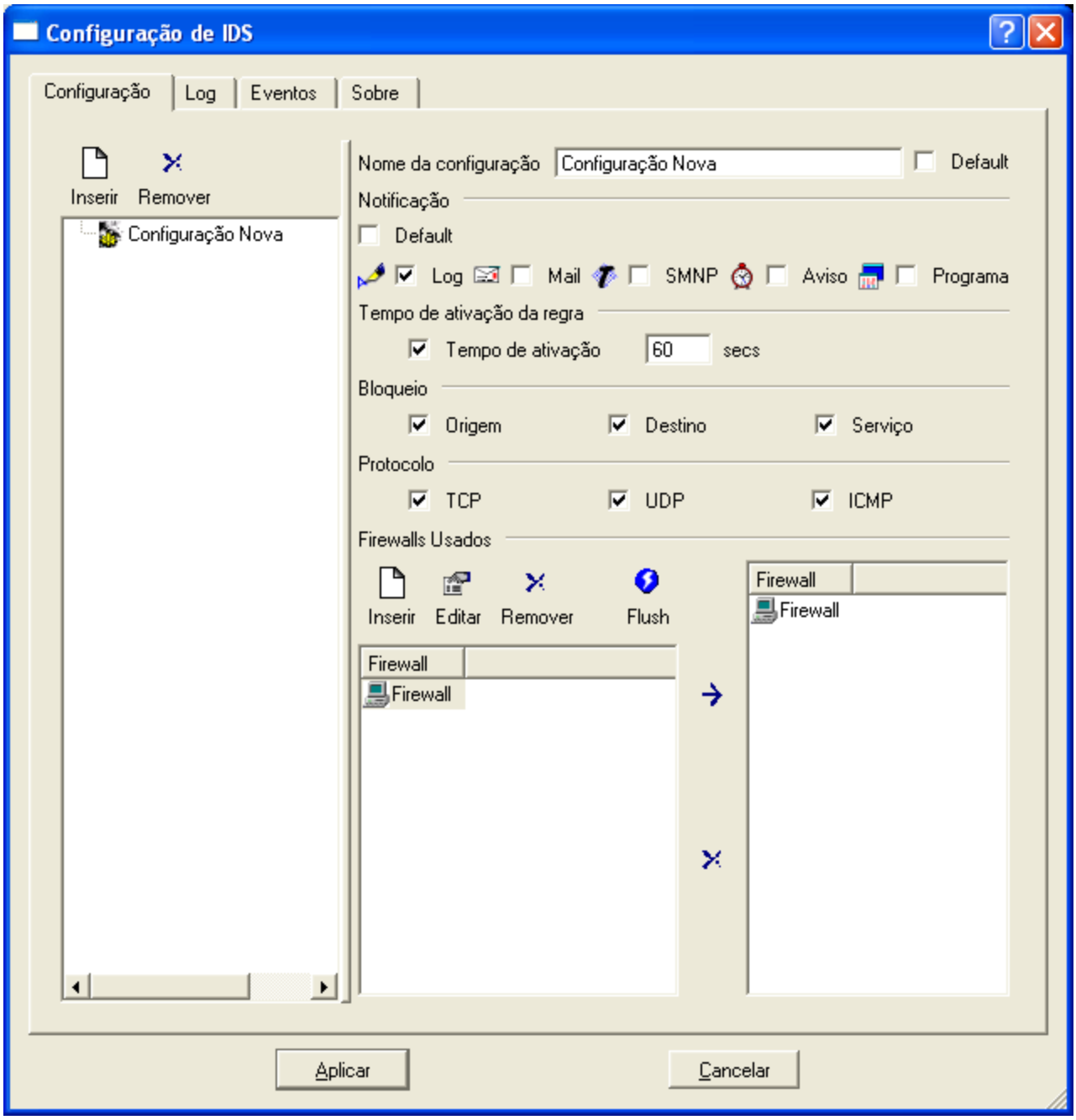
A seguir, deve-se clicar no menu *Iniciar*, selecionar a opção *Executar* e digitar o seguinte comando no campo *Abrir*: `D:\br\firewall\ids\` (caso a unidade de CD-ROM seja diferente de **D**, substituir a letra D, pela letra equivalente). A partir daí, é so escolher a versão correta de acordo com a plataforma desejada e executar o arquivo correspondente.

O programa inicialmente mostrará uma janela pedindo uma confirmação para prosseguir com a instalação. Deve-se clicar no botão **Continuar** para prosseguir com a instalação. A seguir será mostrada uma janela com a licença de uso do produto e pedindo uma confirmação para continuar. Deve-se clicar no botão **Eu Concordo** para dar continuar com a instalação.

Configuração do plugin do Firewall Aker para IDS

Após realizada a instalação do plugin, é necessário se proceder com a sua configuração. Esta configuração permite se fazer o cadastramento de todos os firewalls que serão notificados, bem como a definição de que regras serão acrescentadas.

Para se ter acesso ao programa de configuração deve-se clicar no menu *Iniciar*, selecionar o grupo *Firewall Aker*. Dentro deste selecionar o grupo *Detecção de Intrusão* e então a opção *Detecção de Intrusão*. A seguinte janela será mostrada:



Esta janela consiste de 4 pastas. Na primeira, que está sendo mostrada acima, é onde é feita a configuração do plugin. Ela consiste de uma lista com o nome das diversas configurações criadas pelo administrador e que depois serão mostradas como opção de ação no console de administração do Real Secure. Pode-se especificar o nome de uma das configurações quando na execução de um evento ou utilizar o botão **Default** para se especificar uma configuração que será executada por padrão, isto é, quando não for especificada o nome de nenhuma configuração.

Para se criar uma nova configuração, basta se clicar no botão **Inserir**, localizado na parte esquerda superior da janela. Fazendo-se isso uma configuração em branco será criada. Para se editar os parâmetros desta ou de qualquer outra configuração basta se clicar sobre seu nome e a seguir modificar os parâmetros desejados.

Significado dos parâmetros

Nome da configuração: Este é o nome que será mostrado no console de administração do Real Secure, NFR, Dragon Enterasys e Snort. Quando selecionado, executará as ações definidas pelo administrador.

Notificação: Este campo permite definir que ações serão executadas pelo firewall quando uma regra de bloqueio for acrescentada pela execução da configuração. Caso a opção **Padrão** seja selecionada, então as ações associadas à mensagem *Regra de bloqueio IDS acrescentada* serão executadas. Caso contrário pode-se especificar exatamente que ações devem ser tomadas. Para maiores informações sobre a configuração das ações, veja o capítulo Configurando as ações do sistema.

Bloqueio: Este campo permite se definir que tipo de bloqueio será realizado quando a configuração for executada. Existem três opções possíveis que podem ser selecionadas independentemente (quando mais de uma opção for selecionada, a regra bloqueará pacotes que se enquadrem em todas as opções marcadas e não em apenas algumas):

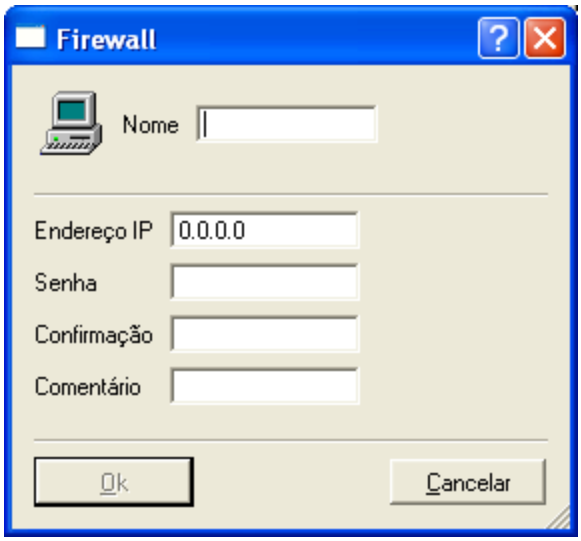
Origem: Os pacotes que tiverem endereço origem igual ao da regra serão bloqueados

Destino: Os pacotes que tiverem endereço destino igual ao da regra serão bloqueados

Serviço: Os pacotes que utilizarem serviço igual ao da regra serão bloqueados. Se esta opção for marcada, deve-se selecionar quais protocolos estarão associados ao serviço através do campo **Protocolo**. Isto é necessário devido a uma limitação do Real Secure na medida em que não fornece o protocolo de um determinado serviço, apenas seu número. Como o NFR inspeciona apenas tráfego TCP, esse protocolo deve ser selecionado no caso desse IDS.

Tempo de ativação da regra: Este campo permite que se defina por quanto tempo as regras acrescentadas por esta configuração ficarão ativas. Caso a opção **Tempo de ativação** esteja marcada, deve-se especificar o tempo, em segundos, que a regra ficará ativa. Caso esta opção não esteja marcada, a regra será mantida até a próxima reinicialização do firewall.

Firewalls Usados: Este campo serve para se definir em quais firewalls as regras temporárias serão acrescentadas. Para cada firewall deve-se configurar uma senha de acesso e seu endereço IP. A senha de acesso deve ser a mesma configurada na definição da entidade do agente IDS (para maiores informações veja o capítulo Cadastrando Entidades). Ao se clicar no botão incluir ou editar, a seguinte janela será mostrada:

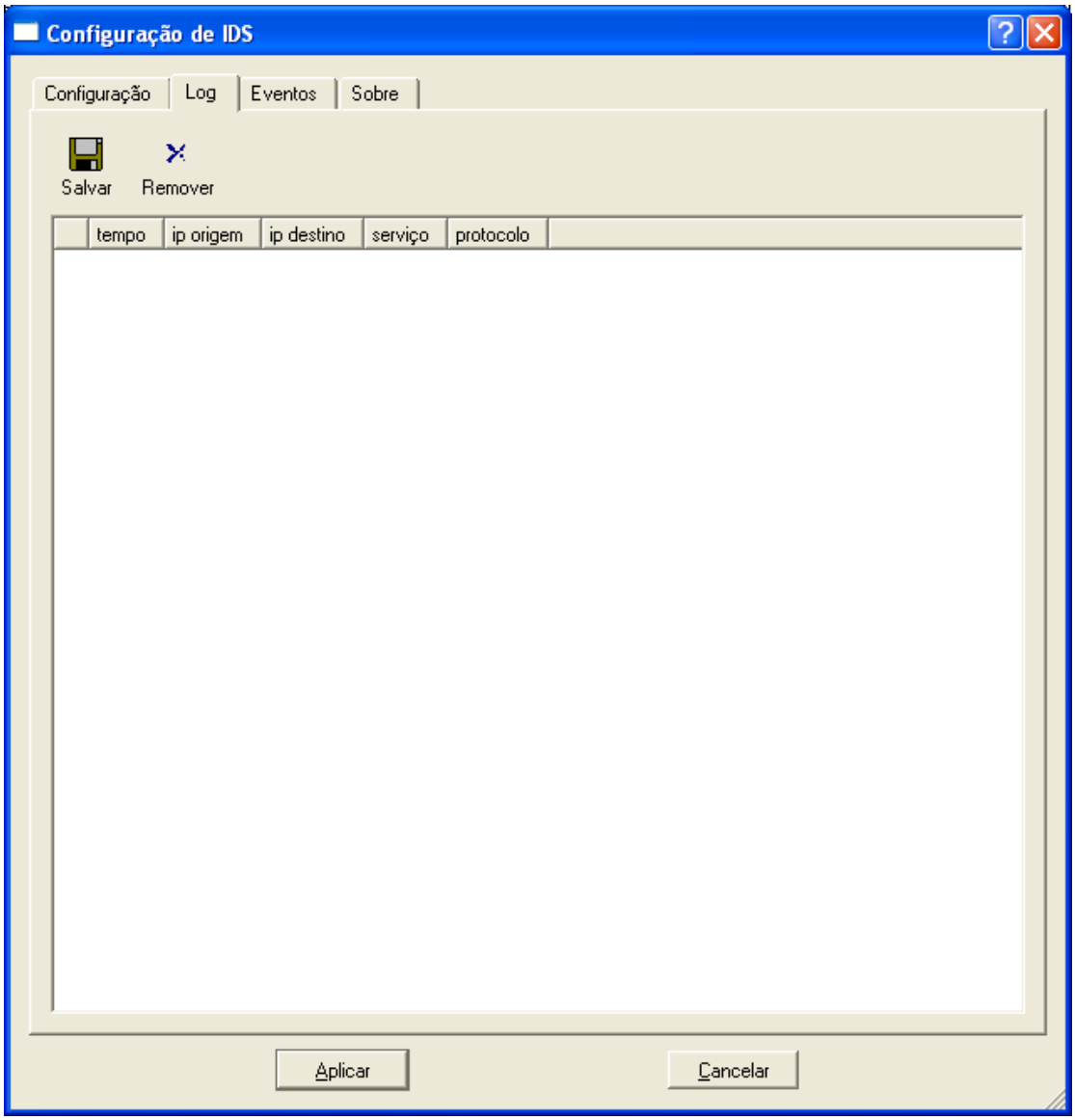


Os firewalls definidos acima devem ser adicionados as configurações fazendo-se os seguintes passos: Selecione os firewalls requeridos; Pressione o botão de seta -> para que os firewall selecionados apareçam na lista da direita da janela.

O botão de **Flush** é utilizado para apagar as regras dinâmicas adicionadas pelos IDS nos firewalls selecionados.

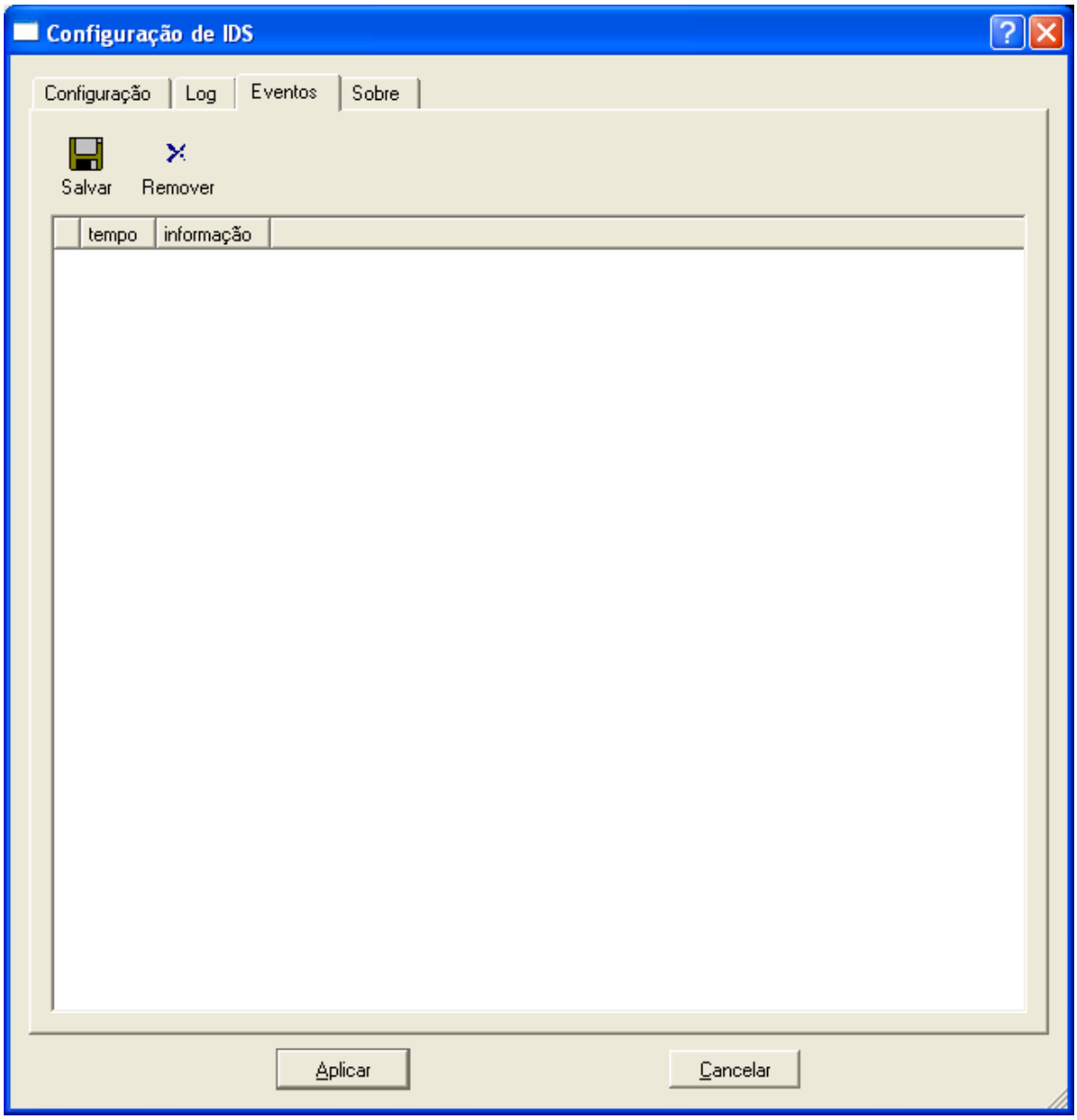
Após se realizar todas as modificações deve-se clicar no botão **Aplicar**. Caso se esteja utilizando o Real Secure será então mostrada uma janela informando que os *Global Responses* do Real Secure serão alterados e pedindo uma confirmação para continuar. Deve-se clicar no botão **Sim** para se salvar a nova configuração.

Log



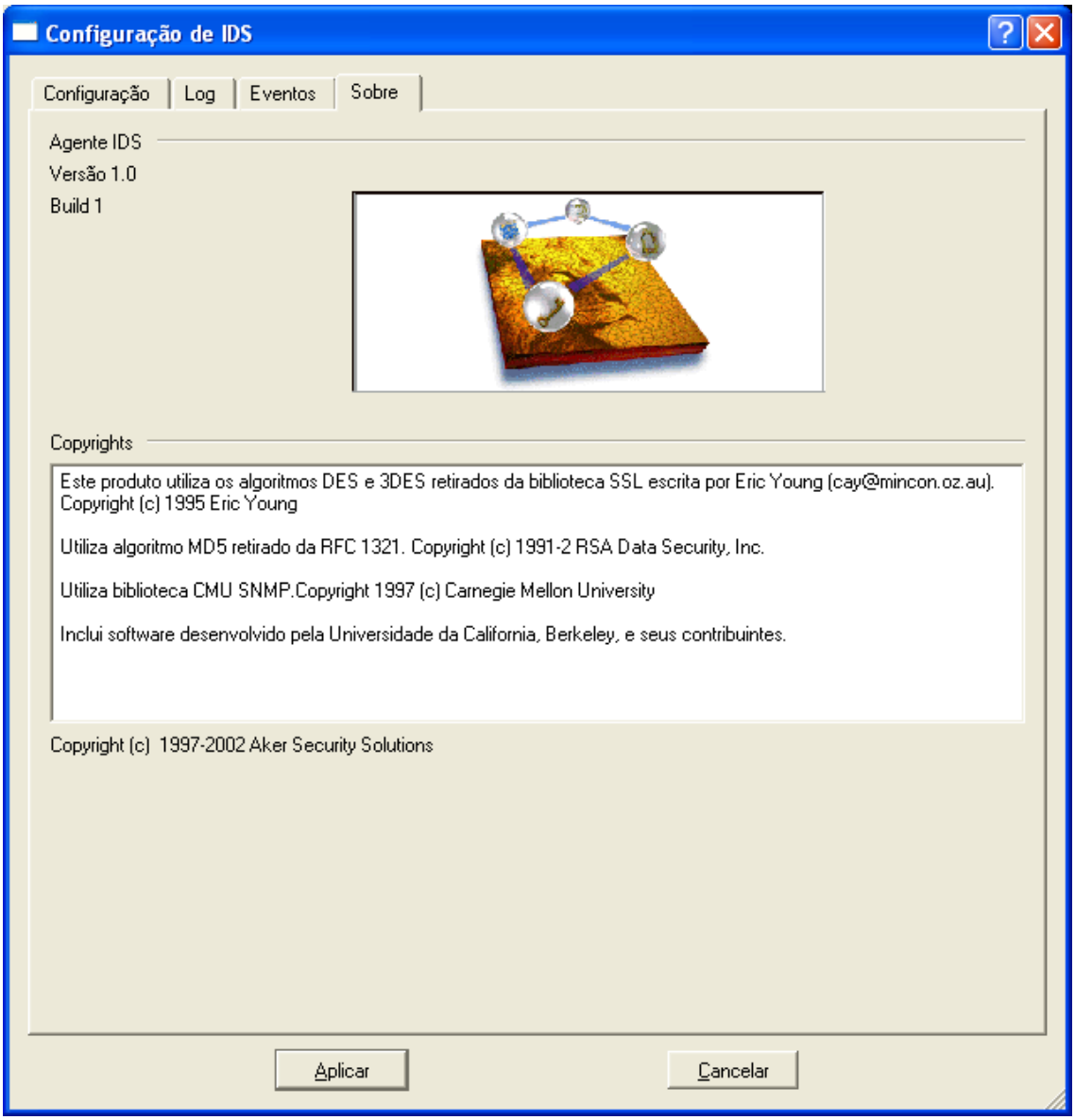
Todos os bloqueios enviados pelo IDS serão registrados nesta janela.

Eventos



Esta pasta é muito útil para se acompanhar o funcionamento do agente. Ela consiste de uma lista com diversas mensagens ordenadas pela hora. Ao lado de cada mensagem existe um ícone colorido, simbolizando sua prioridade.

Sobre


Configuração de IDS
Configuração
Log
Eventos
Sobre
Agente IDS
Versão 1.0
Build 1
Copyrights
Este produto utiliza os algoritmos DES e 3DES retirados da biblioteca SSL escrita por Eric Young (cay@mincon.oz.au). Copyright (c) 1995 Eric Young
Utiliza algoritmo MD5 retirado da RFC 1321. Copyright (c) 1991-2 RSA Data Security, Inc.
Utiliza biblioteca CMU SNMP.Copyright 1997 (c) Carnegie Mellon University
Inclui software desenvolvido pela Universidade da California, Berkeley, e seus contribuintes.
Copyright (c) 1997-2002 Aker Security Solutions
Aplicar
Cancelar

Informações gerais do produto.

12-10 Utilizando a interface texto - Syn Flood

A interface texto de configuração da proteção contra SYN flood é bastante simples de ser usada e tem as mesmas capacidades da interface gráfica.
Localização do programa: `/etc/firewall/fwflood`

Sintaxe:

```
Firewall Aker - Versao 5.1
fwflood - Configura parametros de protecao contra SYN Flood
Uso: fwflood [ativa | desativa | mostra | ajuda]
     fwflood [inclui | remove] <nome>
     fwflood tempo <valor>
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
fwflood - Configura parametros de protecao contra SYN Flood
Uso: fwflood [ativa | desativa | mostra | ajuda]
```

```
     fwflood [inclui | remove] <nome>
     fwflood tempo <valor>
     ativa        = ativa protecao contra SYN Flood
     desativa     = desativa protecao contra SYN Flood
     mostra       = mostra a configuracao atual
     inclui       = inclui uma entidade a ser protegida
     remove       = remove uma das entidades a serem protegidas
     tempo        = configura o tempo maximo de espera para fechar
conexao
     ajuda        = mostra esta mensagem
Para inclui / remove temos:
     nome         = nome da entidade a ser protegida ou removida da
protecao
Para tempo temos:
     valor        = tempo maximo de espera em unidades de 500ms
```

Exemplo 1: (visualizando a configuração)

```
#/etc/firewall/fwflood mostra
Parametros de configuracao:
-------------------------------------
Protecao contra SYN Flood: ativada
Tempo limite de espera   : 6 (x 500 ms)
Lista de entidades a serem protegidas:
-------------------------------------
NT1                                          (Maquina)
NT3                                          (Maquina)
```

12-11 Utilizando a interface texto - Proteção de Flood

Localização do programa: `/etc/firewall/fwmaxconn`

Sintaxe:

```
Firewall Aker - Versao 5.1
Uso: fwmaxconn ajuda
     fwmaxconn mostra
     fwmaxconn inclui <pos> <origem> <destino> <servic> <n_conns>
     fwmaxconn remove <pos>
     fwmaxconn < habilita | desabilita > <pos>
os parametros sao:
        pos     : posicao da regra na tabela
        origem  : maquina/rede de onde se origina as conexoes
        destino : maquina/rede a que se destinam as conexoes
        servico : servico de rede para o qual existe a conexao
        n_conns : numero maximo de conexoes simultaneas de mesma
origem
```

Exemplo 1: (visualizando a configuração)

```
#/etc/firewall/fwmaxconn mostra
Regra 01
--------
Origem   : Rede_Internet
Destino  : NT1
Servicos : HTTP
Conexoes : 5000
Regra 02
--------
Origem   : Rede_Internet
Destino  : NT3
Servicos : FTP
Conexoes : 10000
```

```
Regra 03
--------
Origem   : Rede_Internet
Destino  : Rede_Interna
Servicos : Gopher
Conexoes : 100
```

12-12 Utilizando a interface texto - Anti Spoofing

Localização do programa: `/etc/firewall/fwifnet`
Firewall Aker - Versao 5.1
Uso: fwifnet [ajuda | mostra]
fwifnet inclui interface <nome_if> [externa]
fwifnet inclui rede <nome_if> <rede> [rede1] [rede2] ...
fwifnet remove [-f] interface <nome_if>
fwifnet remove rede <nome_if> <endereco_IP> <mascara>

Ajuda do programa:

```
Uso: fwifnet [ajuda | mostra]
     fwifnet inclui interface <nome_if> [externa]
     fwifnet inclui rede <nome_if> <rede> [rede1] [rede2] ...
     fwifnet remove [-f] interface <nome_if>
     fwifnet remove rede <nome_if> <endereco_IP> <mascara>
para inclui/remove temos:
     interface  : o nome da interface de rede a ser controlada
     externa    : se esta palavra estiver presente, a interface
                  sera' considerada externa pelo firewall
     rede       : uma rede permitida em uma interface nao externa
```

Exemplo 1: (visualizando a configuração)

```
#/etc/firewall/fwifnet mostra
Firewall Aker - Versao 5.1
Status do modulo anti-spoofing: habilitado
Interface cadastrada: Interf_DMZ
      Rede permitida: Rede_DMZ
Interface cadastrada: Interf_externa (externa)
Interface cadastrada: Interf_interna
      Rede permitida: Rede_Interna
```

12-13 Utilizando a interface texto - IDS

A utilização da interface texto na configuração do suporte a detecção de intrusão é bastante simples e possui todos os recursos da interface gráfica.

Localização do programa: `/etc/firewall/fwids`

Sintaxe:

```
fwids [habilita | desabilita | mostra | limpa | ajuda]
fwids agente <entidade>
fwids bloqueia [origem <ip origem>] [destino <ip destino>]
               [servico <servico/protocolo>] [tempo]
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
fwids - Configura parametros do agente IDS externo
Uso: fwids [habilita | desabilita | mostra | limpa | ajuda]
     fwids agente <entidade>
     fwids bloqueia [origem <ip origem>] [destino <ip destino>]
                    [servico <servico/protocolo>] [tempo]
```

```
     habilita     = habilita o funcionamento de agentes IDS externos
     desabilita   = desabilita o funcionamento de agentes IDS externos
     mostra       = mostra a configuracao atual
     bloqueia     = inclui uma regra de bloqueio temporaria
     limpa        = remove todas as regras de bloqueio temporarias
     agente       = especifica nome da entidade com dados do agente
     ajuda        = mostra esta mensagem

Para bloqueia temos:
     origem       = Especifica que deve-se bloquear conexoes
originadas no
                    endereco IP especificado
     destino      = Especifica que deve-se bloquear conexoes
destinadas ao
                    endereco IP especificado
     servico      = Especifica que deve-se bloquear conexoes que
utilizem o
                    servico especificado. Neste caso, deve-se
especificar o
                    servico como a porta, para os protocolos TCP e
UDP, o
                    tipo de servico, para ICMP, ou o numero do
protocolo, no
                    caso de outros protocolos (ex: 23/tcp, 53/udp,
57/outro)
     tempo        = tempo, em segundos, no qual a regra permanecera
ativa. No
                    caso de nao ser especificado, a regra ficara ativa
ate a
                    proxima inicializacao do firewall
```

Exemplo 1: (Habilitando o suporte a detecção de intrusão)

```
#/etc/firewall/fwids habilita
```

Exemplo 2: (Definindo o agente IDS)

```
#/etc/firewall/fwids agente Agente_IDS
```

A entidade *Agente_IDS* deve ter sido previamente cadastrada no sistema. Para maiores informações sobre como cadastrar entidades no Firewall Aker, veja o capítulo entitulado Cadastrando Entidades.

Exemplo 3: (Mostrando a configuração atual)

```
#/etc/firewall/fwids mostra
Parametros de configuracao:
---------------------------
Agente IDS externo: habilitado
Agente: Agente_IDS
```

Exemplo 4: (Acrescentando uma regra de bloqueio da máquina 192.168.0.25 para a máquina 10.0.0.38, no serviço WWW, porta 80 do protocolo TCP, por uma hora)

```
#/etc/firewall/fwids bloqueia origem 192.168.0.25 destino 10.0.0.38
servico 80/tcp 3600
```

13-0 Configurando as Ações do Sistema

Neste capítulo mostraremos como configurar as respostas automáticas do sistema para situações pré-determinadas.

O que são as ações do sistema ?

O Firewall Aker possui um mecanismo que possibilita a criação de respostas automáticas para determinadas situações. Estas respostas automáticas são configuradas pelo administrador em uma série de possíveis ações independentes que serão executadas quando uma situação pré-determinada ocorrer.

Para que servem as ações do sistema ?

O objetivo das ações é possibilitar um alto grau de interação do Firewall com o administrador. Com o uso delas, é possível, por exemplo, que seja executado um programa capaz de chamá-lo através de um pager quando a máquina detectar que um ataque está em andamento. Desta forma, o administrador poderá tomar uma ação imediata, mesmo que ele não esteja no momento monitorando o funcionamento do Firewall.

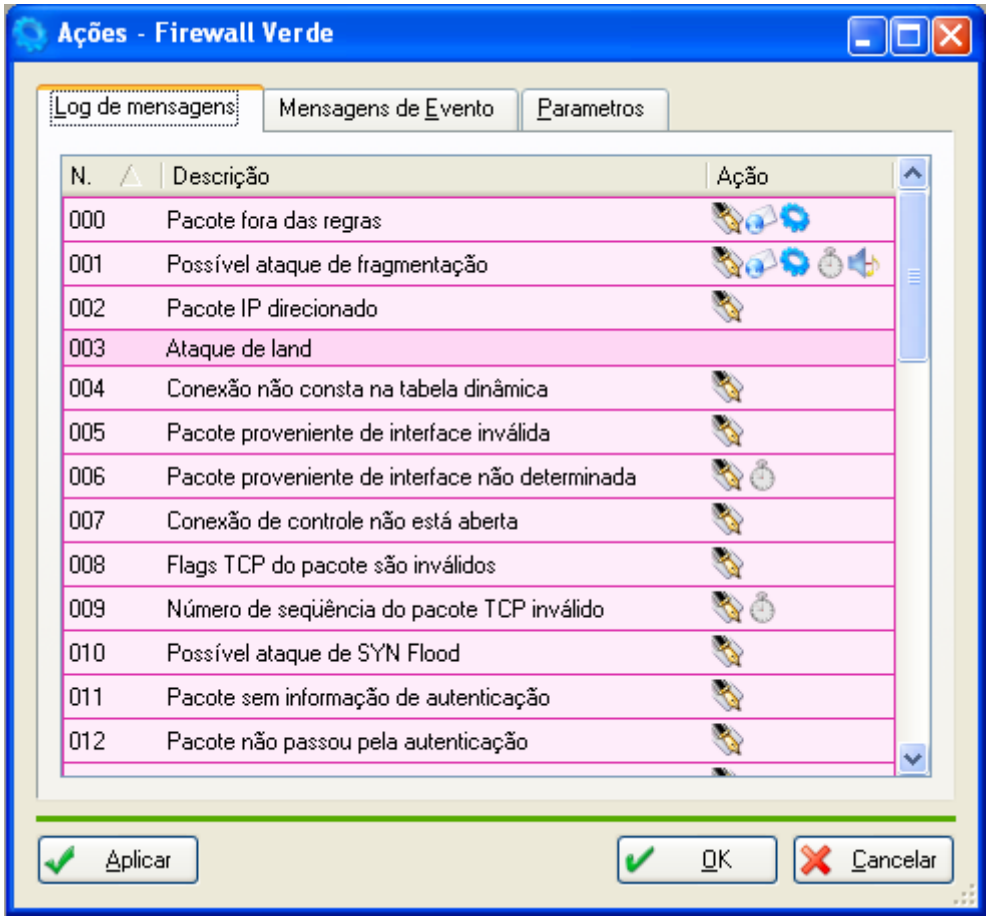
13-1 Utilizando a interface gráfica

Para ter acesso a janela de configuração das ações basta:

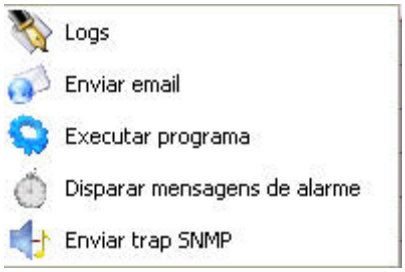
- Expandir o ítem *Configurações do Sistema*
- Selecionar o item *Ações*

A janela de configuração das ações

Ao se selecionar esta opção será mostrada a janela de configuração das ações a serem executadas pelo sistema. Para cada mensagem de log e de eventos e para os pacotes que não se enquadrarem em nenhuma regra é possível se determinar ações independentes. A janela mostrada terá a seguinte forma:


Ações - Firewall Verde
Log de mensagens
Mensagens de Evento
Parametros
N.
Descrição
Ação
000 Pacote fora das regras
001 Possível ataque de fragmentação
002 Pacote IP direcionado
003 Ataque de land
004 Conexão não consta na tabela dinâmica
005 Pacote proveniente de interface inválida
006 Pacote proveniente de interface não determinada
007 Conexão de controle não está aberta
008 Flags TCP do pacote são inválidos
009 Número de seqüência do pacote TCP inválido
010 Possível ataque de SYN Flood
011 Pacote sem informação de autenticação
012 Pacote não passou pela autenticação
Aplicar
OK
Cancelar

Para selecionar as ações a serem executadas para as mensagens mostradas na janela, basta se clicar com o botão direito do mouse sobre as mensagens. A cada opção selecionada aparecerá um ícone correspondente.



Se a opção estiver marcada com o ícone aparente, a ação correspondente será executada pelo Firewall quando a mensagem ocorrer. São permitidas as seguintes ações:

- **Logs**: Se esta opção estiver selecionada, todas as vezes que a mensagem correspondente ocorrer, ela será registrada pelo firewall.
- **Enviar email**: Se esta opção estiver selecionada, será enviado um e-mail todas as vezes que a mensagem correspondente ocorrer (a configuração do endereço de e-mail será mostrada no próximo tópico).
- **Executar programa**: Se esta opção estiver marcada, será executado um programa definido pelo administrador todas as vezes que a mensagem correspondente ocorrer (a configuração do nome do programa a ser executado será mostrada no próximo tópico).

- **Disparar mensagens de alarme**: Se esta opção estiver selecionada, o firewall mostrará uma janela de alerta todas as vezes que a mensagem correspondente ocorrer. Esta janela de alerta será mostrada na máquina onde a interface gráfica remota estiver aberta e, se a máquina permitir, será emitido também um aviso sonoro. Caso a interface gráfica não esteja aberta, não será mostrada nenhuma mensagem e esta opção será ignorada (esta ação é particularmente útil para chamar a atenção do administrador quando ocorrer uma mensagem importante).
- **Enviar trap SNMP**: Se esta opção estiver selecionada, será enviada uma Trap SNMP para o gerente SNMP todas as vezes que a mensagem correspondente ocorrer (a configuração dos parâmetros de configuração para o envio das traps será mostrada no próximo tópico).

Não é possível alterar as ações para a mensagem de inicialização do firewall (mensagem número 43). Esta mensagem sempre terá como ações configuradas apenas a opção Loga.

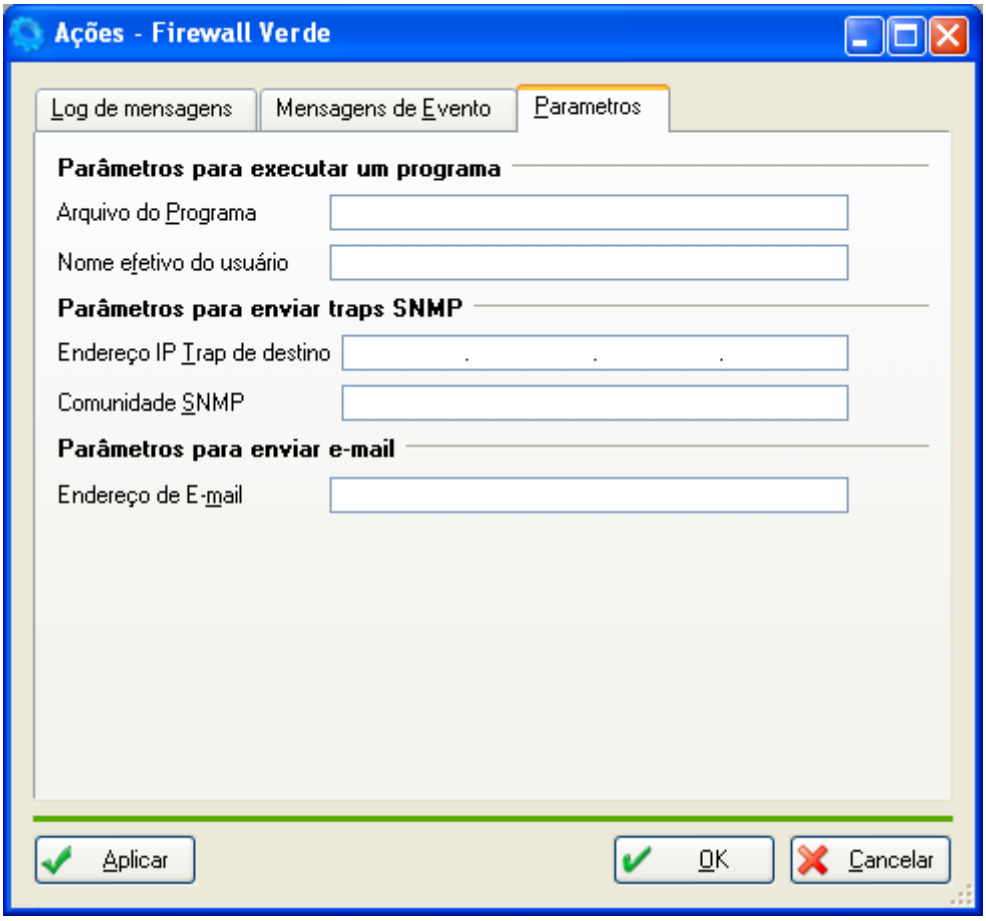
Significado dos botões da janela de ações

- O botão **OK** fará com que a janela de ações seja fechada e as alterações efetuadas aplicadas.
- O botão **Cancelar** fará com que a janela seja fechada porém as alterações efetuadas não serão aplicadas.
- O botão **Aplicar**, fará com que as alterações sejam aplicadas sem que a janela feche.

A janela de configuração dos parâmetros

Para que o sistema consiga executar as ações, é necessário que se configure certos parâmetros (por exemplo, para o Firewall enviar um e-mail, é necessário se configurar o endereço). Estes parâmetros são configurados através da janela de configuração de parâmetros para as ações.

Esta janela é mostrada ao se selecionar **Parâmetros** na janela de Ações. Ela tem o seguinte formato:



Significado dos parâmetros:

- **Parâmetros para executar um programa**

Programa externo: Este parâmetro configura o nome do programa que será executado pelo sistema quando ocorrer uma ação marcada com a opção *Programa*. Deve ser colocado o nome completo do programa, incluindo o caminho. Deve-se atentar para o fato de que o programa e todos os diretórios do caminho devem ter permissão de execução pelo usuário que irá executá-lo (que é configurado na próxima opção).

O programa receberá os seguintes parâmetros pela linha de comando (na ordem em que serão passados):

1. Nome do próprio programa sendo executado (isto é um padrão do sistema operacional Unix).
2. Tipo de mensagem (**1** - para log ou **2**- para evento).
3. Prioridade (**7** - depuração, **6** - informação, **5** - notícia, **4** - advertência ou **3** - erro).
4. Número da mensagem que provocou a execução do programa ou **0** para indicar a causa não foi uma mensagem. (neste caso, a execução do programa foi motivada por uma regra)
5. Cadeia de caracteres ASCII com o texto completo da mensagem (esta cadeia de caracteres pode conter o caractere de avanço de linha no meio dela).

No sistema operacional UNIX, usa-se a barra "/" para especificar o caminho de um programa. Isto pode causar confusão para quem estiver acostumado com o ambiente DOS/Windows, que usa a barra invertida "\".

Nome de usuário efetivo: Este parâmetro indica a identidade com a qual o programa externo será executado. O programa terá os mesmos privilégios deste usuário.

Este usuário deve ser um usuário válido, cadastrado no FreeBSD ou Linux. Não se deve confundir com os usuários do Firewall Aker, que servem apenas para a administração do Firewall.

- **Parâmetros para enviar traps SNMP**

Endereço IP do servidor SNMP: Este parâmetro configura o endereço IP da máquina gerente SNMP para a qual o firewall deve enviar as traps.

Comunidade SNMP: Este parâmetro configura o nome da comunidade SNMP que deve ser enviada nas traps.

As traps SNMP enviadas terão o tipo genérico **6** (*enterprise specific*) e o tipo específico **1** para log ou **2** para eventos. Elas serão enviadas com o número de empresa (*enterprise number)* **2549**, que é o número designado pela IANA para a Aker Consultoria e Informática.

Existe um arquivo chamado **/etc/firewall/mibs/AKER-MIB.TXT** que traz as informações sobre a sub-árvore da Aker Consultoria e Informática na árvore global. Este arquivo está escrito na notação ASN.1.

- **Parâmetros para enviar e-mail**

Endereço de e-mail: Este parâmetro configura o endereço de e-mail do usuário para o qual devem ser enviados os e-mails. Este usuário pode ser um usuário da própria máquina ou não (neste caso deve-se colocar o endereço completo, por exemplo user@aker.com.br).

Caso se deseje enviar e-mails para vários usuários, pode-se criar uma lista e colocar o nome da lista neste campo.

É importante notar que caso algum destes parâmetros esteja em branco, a ação correspondente não será executada, mesmo que ela esteja marcada para tal.

13-2 Utilizando a interface texto

A interface texto para a configuração das ações possui as mesmas capacidades da interface gráfica e é de fácil uso.

Localização do programa: `/etc/firewall/fwaction`

Sintaxe:

```
fwaction ajuda
fwaction mostra
fwaction atribui <numero> [loga] [mail] [trap] [programa] [alerta]
fwaction <programa | usuario | comunidade> [nome]
fwaction ip [endereco IP]
fwaction e-mail [endereco]
```

Ajuda do programa:

```
fwaction - Interface texto para a configuracao das acoes do sistema
Uso: fwaction ajuda
     fwaction mostra
     fwaction atribui <numero> [loga] [mail] [trap] [programa]
[alerta]

     fwaction <programa | usuario | comunidade> [nome]
     fwaction ip [endereco IP]
     fwaction e-mail [endereco]

     ajuda      = mostra esta mensagem
     mostra     = lista as mensagens e as acoes configuradas para cada
uma
     atribui    = configura as acoes para uma determinada mensagem
     programa   = define o nome do programa a ser executado
     usuario    = define o nome do usuario que executara o programa
     comunidade = define o nome da comunidade SNMP para o envio das
traps
     ip         = define o endereco IP do servidor SNMP que recebera
as traps
     e-mail     = define o nome do usuario que recebera os e-mails

Para atribui temos:
     numero   = numero da mensagem a atribuir as acoes
                (o numero de cada mensagem aparece na esquerda ao se
                 selecionar a opcao mostra)
     loga      = Loga cada mensagem que for gerada
     mail      = Manda um e-mail para cada mensagem que for gerada
     trap      = Gera trap SNMP para cada mensagem que for gerada
     programa  = Executa programa para cada mensagem que for gerada
     alerta    = Abre janela de alerta para cada mensagem que for
gerada
```

Exemplo 1: (configurando os parâmetros para envio de e-mail e execução de programa)

```
#fwaction e-mail root
#fwaction programa /etc/pager
#fwaction usuario nobody
```

Exemplo 2: (mostrando a configuração completa das ações do sistema)

```
#fwaction mostra
Condicoes Gerais:

00 - Pacote fora das regras
>>>> Loga

Mensagens do log:
```

```
01 - Possivel ataque de fragmentacao
>>>> Loga
02 - Pacote IP direcionado
>>>> Loga
03 - Ataque de land
>>>> Loga
04 - Conexao nao consta na tabela dinamica
>>>> Loga
05 - Pacote proveniente de interface invalida
>>>> Loga
06 - Pacote proveniente de interface nao determinada
>>>> Loga
07 - Conexao de controle nao esta aberta
>>>> Loga

(...)

237 - O Secure Roaming encontrou um erro
>>>> Loga
238 - O Secure Roaming encontrou um erro fatal
>>>> Loga
239 - Usuarios responsaveis do Configuration Manager
>>>> Loga

Parametros de configuracao:

programa  : /etc/pager
usuario   : nobody
e-mail    : root
comunidade:
ip        :
```

Atenção: Devido ao grande número de mensagens, só estão sendo mostradas as primeiras e as últimas. O programa real mostrará todas ao ser executado.

Exemplo 3: (atribuindo as ações para os *Pacotes fora das regras* e mostrando as mensagens)

```
#fwaction atribui 0 loga mail alerta
#fwaction mostra
Condicoes Gerais:

00 - Pacote fora das regras
>>>> Loga Mail Alerta

Mensagens do log:

01 - Possivel ataque de fragmentacao
>>>> Loga
02 - Pacote IP direcionado
>>>> Loga
03 - Ataque de land
>>>> Loga
04 - Conexao nao consta na tabela dinamica
>>>> Loga
05 - Pacote proveniente de interface invalida
>>>> Loga
06 - Pacote proveniente de interface nao determinada
>>>> Loga
```

```
07 - Conexao de controle nao esta aberta
>>>> Loga

(...)

237 - O Secure Roaming encontrou um erro
>>>> Loga
238 - O Secure Roaming encontrou um erro fatal
>>>> Loga
239 - Usuarios responsaveis do Configuration Manager
>>>> Loga


Parametros de configuracao:

programa  : /etc/pager
usuario   : nobody
e-mail    : root
comunidade:
ip        :
```

Atenção: Devido ao grande número de mensagens, só estão sendo mostradas as primeiras e as últimas. O programa real mostrará todas ao ser executado.

Exemplo 4: (cancelando todas as ações para a mensagem de *Pacote IP direcionado* e mostrando as mensagens)

```
#fwaction atribui 2
#fwaction mostra
Condicoes Gerais:

00 - Pacote fora das regras
>>>> Loga Mail Alerta

Mensagens do log:

01 - Possivel ataque de fragmentacao
>>>> Loga Mail
02 - Pacote IP direcionado
>>>>
03 - Ataque de land
>>>> Loga
04 - Conexao nao consta na tabela dinamica
>>>> Loga
05 - Pacote proveniente de interface invalida
>>>> Loga
06 - Pacote proveniente de interface nao determinada
>>>> Loga
07 - Conexao de controle nao esta aberta
>>>> Loga

(...)

237 - O Secure Roaming encontrou um erro
>>>> Loga
238 - O Secure Roaming encontrou um erro fatal
>>>> Loga
239 - Usuarios responsaveis do Configuration Manager
>>>> Loga
```

```
Parametros de configuracao:

programa  : /etc/pager
usuario   : nobody
e-mail    : root
comunidade:
ip        :
```

Atenção: Devido ao grande número de mensagens, só estão sendo mostradas as primeiras e as últimas. O programa real mostrará todas ao ser executado.

14-0 Visualizando o log do Sistema

Neste capítulo mostraremos como visualizar o log do sistema, um recurso imprescindível na detecção de ataques, no acompanhamento e monitoramento do firewall e na fase de configuração do sistema.

O que é o log do sistema ?

O log é o local onde o firewall guarda todas as informações relativas aos pacotes recebidos. Nele podem aparecer registros gerados por qualquer um dos três grandes módulos: filtro de pacotes, conversor de endereços e criptografia/autenticação. O tipo de informação guardada no log depende da configuração realizada no firewall, mas basicamente ele inclui informações sobre os pacotes que foram aceitos, descartados e rejeitados, os erros apresentados por certos pacotes e as informações sobre a conversão de endereços.

De todos estes dados, as informações sobre os pacotes descartados e rejeitados é possivelmente a de maior importância, já que é através delas que se consegue determinar possíveis tentativas de invasão, tentativa de uso de serviços não autorizados, erros de configuração, etc.

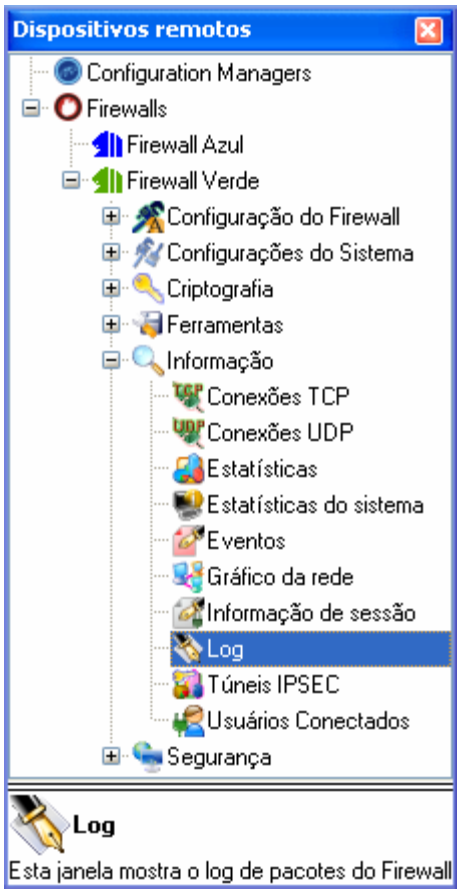
O que é um filtro de log ?

Mesmo que o sistema tenha sido configurado para registrar todo o tipo de informação, muitas vezes se está interessado em alguma informação específica (por exemplo, suponha que se deseje ver as tentativas de uso do serviço POP3 de uma determinada máquina que foram rejeitadas em um determinado dia, ou ainda, quais foram aceitas). O filtro de log é um mecanismo oferecido pelo Firewall Aker para se criar visões do conjunto total de registros, possibilitando que se obtenha as informações desejadas facilmente.

O filtro só permite a visualização de informações que tiverem sido registradas no log. Caso se deseje obter uma determinada informação, é necessário inicialmente configurar o sistema para registrá-la e então utilizar um filtro para visualizá-la.

14-1 Utilizando a interface gráfica

Para ter acesso a janela de visualização do log basta:



- Clicar no menu *Informação* do firewall que se deseja ver o log
- Selecionar a opção *Log*

A barra de ferramentas do Log

Todas as vezes que se seleciona a opção *Log*, é mostrada automaticamente a barra de ferramentas de Log. Esta barra, que estará ao lado das outras barras, poderá ser arrastada e ficar flutuando acima das informações do Log. Ela tem o seguinte formato:

Significado dos Ícones:

Abre a janela de filtragem do firewall

Este ícone somente irá aparecer quando o firewall estiver fazendo uma procura no Log. Ele permite interromper a busca do firewall

Exporta o log para diversos formatos de arquivos

Apaga o Log do firewall

Realiza uma resolução reversa dos IP que estão sendo mostrados pelo Log

Permite fazer uma atualização da tela de logs dentro de um determinado período definido no campo seguinte

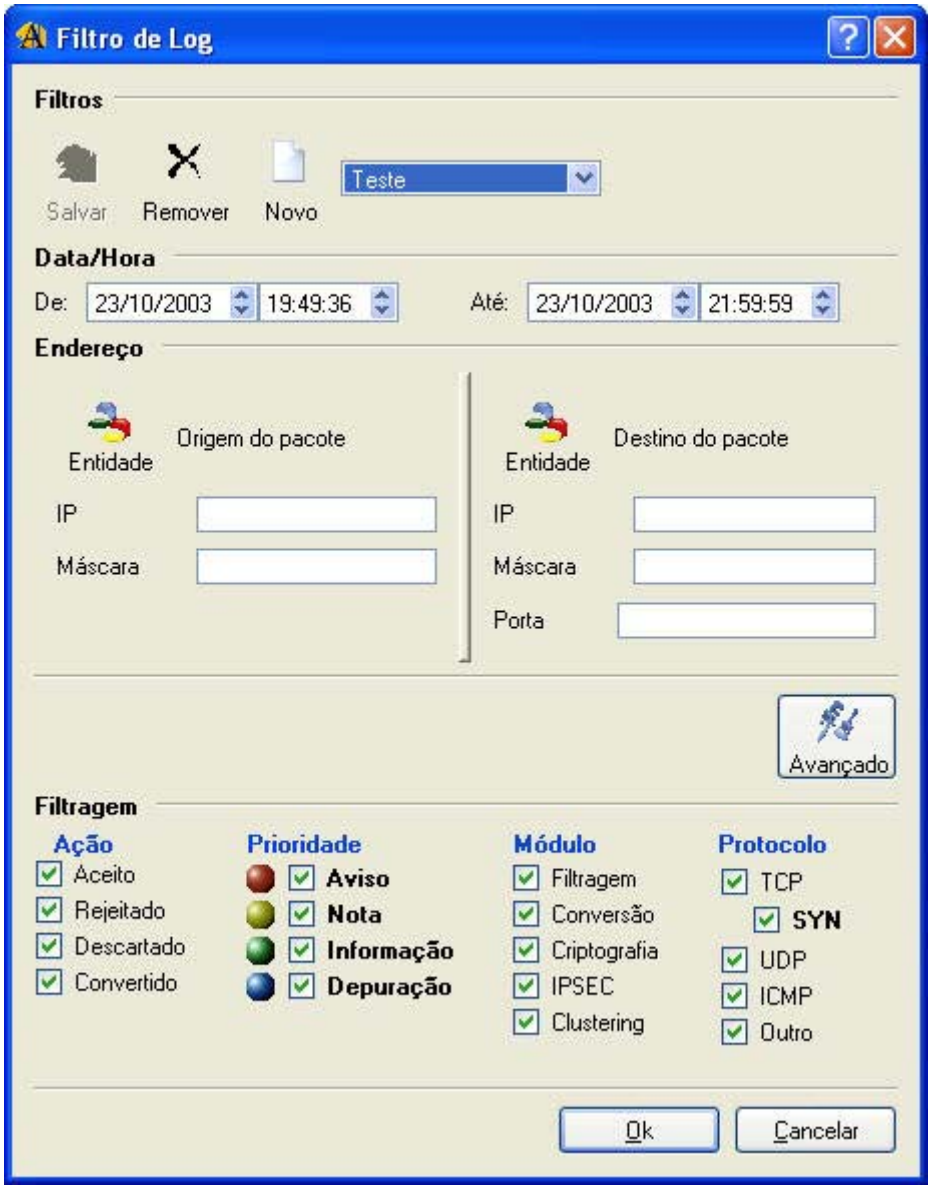
Define o tempo que o firewall irá atualizar a janela com informações de log

Percorre o Log para frente e para trás

Expande as mensagens de Log, mostrando as mesmas com o máximo de informação

Ao clicar no ícone de filtro a janela abaixo irá aparecer:

A Janela de Filtragem de Log



Na parte superior da janela, encontram-se os botões **Salvar**, **Remover e Novo**. Permite gravar um perfil de pesquisa que poderá ser usado posteriormente pelo administrador.

Para salvar um filtro de log, deve-se proceder da seguinte forma:

1. Preenche-se todos os seus campos da forma desejada
2. Define-se, no campo **Filtros**, o nome pelo qual ele será referenciado.
3. Clica-se no botão Salvar.

Para se aplicar um filtro salvo, basta selecionar seu nome no campo **Filtros** e todos os campos serão automaticamente preenchidos com os dados salvos.

Para excluir um filtro que não mais seja desejado, deve-se proceder da seguinte forma:

1. Seleciona-se o filtro a ser removido, no campo **Filtros**.

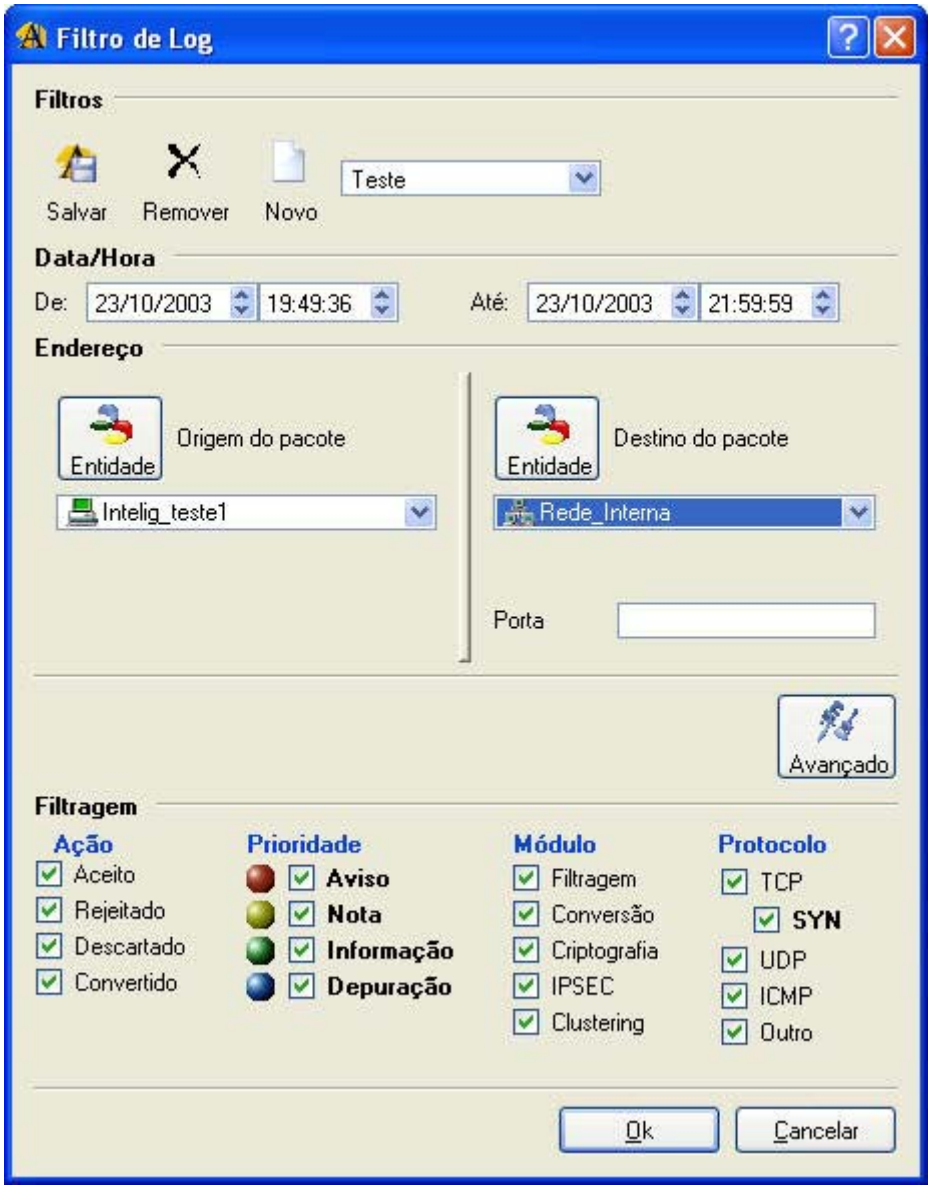
2. Clica-se no botão Remover.

O filtro padrão é configurado para mostrar todos os registros do dia atual. Para se alterar a visualização para outros dias, na janela **Data/Hora**, pode-se configurar os campos **De** e **Para** para os dias desejados (a faixa de visualização compreende os registros da data inicial à data final, inclusive).

Caso se deseje ver os registros cujos endereços origem e/ou destino do pacote pertençam a um determinado conjunto de máquinas, pode-se utilizar os campos IP / Máscara ou Entidade para especificá-lo.

O botão

permitem a escolha do modo de filtragem a ser realizado: caso o botão esteja selecionado, serão mostrados na janela os campos, chamados de **IP** , **Máscara (para origem do pacote) e IP** , **Máscara (para Destino do pacote)**. Estes campos poderão ser utilizados para especificar o conjunto origem e/ou o conjunto destino. Neste caso, pode-se selecionar uma entidade em cada um destes campos e estas serão utilizadas para especificar os conjuntos origem e destino. O botão pode ser usado independente um do outro, ou seja posso escolher selecionar pela entidade na origem e por IP e Máscara para o destino.



Para monitorar um serviço específico, basta colocar seu número no campo **Porta**. A partir deste momento só serão mostradas entradas cujo o serviço especificado for utilizado. É importante também que se selecione o protocolo correspondente ao serviço desejado no campo protocolo, mostrado abaixo.

No caso dos protocolos TCP e UDP, para se especificar um serviço, deve-se colocar o número da porta destino, associada ao serviço, neste campo. No caso do ICMP deve-se colocar o tipo de serviço. Para outros protocolos, coloca-se o número do protocolo desejado.

Além destes campos, existem outras opções que podem ser combinadas para restringir ainda mais o tipo de informação mostrada:

Ação:

Representa que ação o sistema tomou ao lidar com o pacote em questão. Existem as seguintes opções possíveis, que podem ser selecionadas independentemente:

- Aceito

Mostra os pacotes que foram aceitos pelo firewall.

- Rejeitado

Mostra os pacotes que foram rejeitados pelo firewall.

- Descartado

Mostra os pacotes que foram descartados pelo firewall.

- Convertido

Mostra as mensagens relacionadas à conversão de endereços.

Prioridade:

Diferentes tipos de mensagens possuem prioridades diferentes. Quanto maior for a prioridade associada a um determinado registro, mais importância deve-se dar a ele. Abaixo está a lista com as todas as prioridades possíveis, ordenada da mais importante para a menos (caso tenha se configurado o firewall para mandar uma cópia do log para o syslogd, as prioridades com as quais as mensagens serão geradas no syslog são as mesmas apresentadas abaixo):

- Aviso

Os registros que se enquadram nesta prioridade normalmente indicam que algum tipo de ataque ou situação bastante séria (como por exemplo, um erro na configuração dos fluxos de criptografia) está ocorrendo. Este tipo de registro sempre vem precedido de uma mensagem que fornece maiores explicações sobre ele.

- Nota

Normalmente se enquadram nesta prioridade os pacotes que foram rejeitados ou descartados pelo sistema, em virtude destes terem se encaixado em uma regra configurada para rejeitá-los ou descartá-los ou por não terem se encaixado em nenhuma regra. Em algumas situações eles podem ser precedidos por mensagens explicativas.

- Informação

Os registros desta prioridade acrescentam informações úteis mas não tão importantes para a administração do Firewall. Estes registros nunca são precedidos por mensagens explicativas. Normalmente se enquadram nesta prioridade os pacotes aceitos pelo firewall.

- Depuração

Os registros desta prioridade não trazem nenhuma informação realmente útil, exceto quando se está configurando o sistema. Se enquadram nesta prioridade as mensagens de conversão de endereços.

Módulo:

Esta opção permite visualizar independentemente os registros gerados por cada um dos três grandes módulos do sistema: filtro de pacotes, conversor de endereços, módulo de criptografia, IPSEC e Clustering.

Protocolo:

Este campo permite que se especifique o protocolo dos registros a serem mostrados. As seguintes opções são permitidas:

- TCP

Serão mostrados os registros gerados a partir de pacotes TCP. Se esta opção for marcada, a opção TCP/SYN será automaticamente desmarcada.

- TCP/SYN

Serão mostrados os registros gerados a partir de pacotes TCP de abertura de conexão (pacotes com o flag de SYN ativo). Se esta opção for marcada, a opção TCP será automaticamente desmarcada.

- UDP

Serão mostrados os registros gerados a partir de pacotes UDP.

- ICMP

Serão mostrados os registros gerados a partir de pacotes ICMP.

- Outro

Serão mostrados registros gerados a partir de pacotes com protocolo diferente de TCP, UDP e ICMP. Pode-se restringir mais o protocolo a ser mostrado, especificando seu número através do campo **Porta destino ou Tipo de Serviço.**

- O botão **OK** aplicará o filtro escolhido e mostrará a janela de log, com as informações selecionadas.
- O botão **Cancelar** fará com que a operação de filtragem seja cancelada e a janela de log mostrada com as informações anteriores.

A janela de log

Log - Firewall Verde
Data Hora Repetição Ação Protocolo Status IP de origem Porta de origem IP de destino Porta de destino Flags Interface
10/23/2003 21:54:01 1 D UDP 192.168.1.4 138 192.168.1.255 138 Inc0
Pacote proveniente de interface inválida
10/23/2003 21:51:25 1 A TCP 192.168.1.15 1590 192.168.1.45 1020 S Inc1
10/23/2003 21:42:00 1 D UDP 192.168.1.4 138 192.168.1.255 138 Inc0
Pacote proveniente de interface inválida
10/23/2003 21:38:31 6 D UDP 192.168.1.15 137 192.168.1.255 137 Inc0
Pacote proveniente de interface inválida
10/23/2003 21:37:17 3 D UDP 192.168.1.4 137 192.168.1.255 137 Inc0
Pacote proveniente de interface inválida
10/23/2003 21:37:16 2 D UDP 192.168.1.1 138 192.168.1.255 138 Inc0
Pacote proveniente de interface inválida
10/23/2003 21:37:06 1 D UDP 192.168.1.3 138 192.168.1.255 138 Inc0
Pacote proveniente de interface inválida
10/23/2003 21:37:05 3 D UDP 192.168.1.4 137 192.168.1.255 137 Inc0
Pacote proveniente de interface inválida
Módulo:
Prioridade:
Regra:
Aplicar
OK
Cancelar

A janela de log será mostrada após a aplicação de um filtro novo. Ela consiste de uma lista com várias entradas. Todas as entradas possuem o mesmo formato, entretanto, dependendo do protocolo do pacote que as gerou, alguns campos podem estar ausentes. Além disso, algumas entradas serão precedidas por uma mensagem especial, em formato de texto, que trará informações adicionais sobre o registro (o significado de cada tipo de registro será mostrado no próximo tópico).

Observações importantes:

- Os registros serão mostrados de 100 em 100.
- Só serão mostrados os primeiros 10.000 registros que se enquadrem no filtro escolhido. Os demais podem ser vistos exportando o log para um arquivo ou utilizando um filtro que produza um número menor de registros.
- No lado esquerdo de cada mensagem, será mostrado um ícone colorido simbolizando sua prioridade. As cores tem o seguinte significado:

Azul	Depuração
Verde	Informação
Amarelo	Nota
Vermelho	Aviso

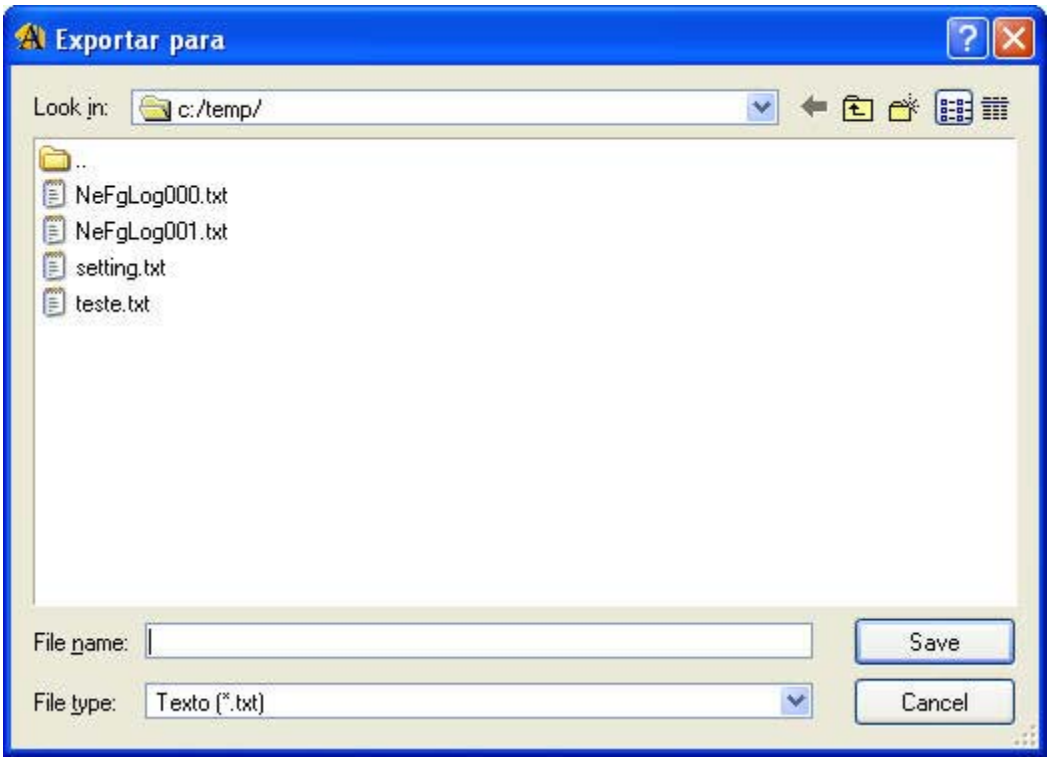
- Ao se clicar com o botão esquerdo sobre uma mensagem, aparecerá na parte inferior da tela uma linha com informações adicionais sobre o registro.

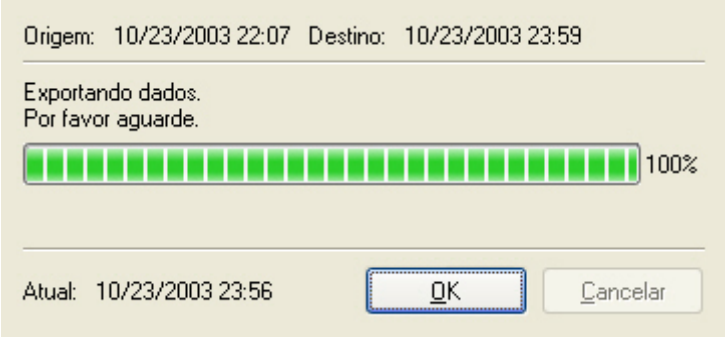
Ao se apagar todo o log, não existe nenhuma maneira de se recuperar as informações anteriores. A única possibilidade de recuperação é a restauração de uma cópia de segurança.

Se a opção *Expande mensagens* estiver marcada e se tiver escolhido a opção de exportação em formato texto, o log será exportado com as mensagens complementares; caso contrário, o log será exportado sem elas.

Esta opção é bastante útil para se enviar uma cópia do log para alguma outra pessoa, para se guardar uma cópia em formato texto de informações importantes ou para se

importar o log por um analisadores de log citados acima. Ao ser clicado, será mostrada a seguinte janela:





Para exportar o conteúdo do log, basta fornecer o nome do arquivo a ser criado, escolher seu formato e clicar no botão **Salvar**. Para cancelar a operação, clique em **Cancelar**.

Se já existir um arquivo com o nome informado ele será apagado.

- O botão **Próximos**, representado como uma seta para a direita na barra de ferramentas, mostrará os próximos 100 registros selecionados pelo filtro. Se não existirem mais registros, esta opção estará desabilitada.
- O botão **Últimos**, representado como uma seta para a esquerda na barra de ferramentas, mostrará os 100 registros anteriores. Se não existirem registros anteriores, esta opção estará desabilitada.
- O botão **Ajuda** mostrará a janela de ajuda específica para a janela de log.

14-2 Formato e significado dos campos dos registros do log

Abaixo segue a descrição do formato de cada registro, seguido de uma descrição de cada um dos campos. O formato dos registros é o mesmo para a interface gráfica e para a interface texto.

Registros gerados pelo filtro de pacotes ou pelo módulo de criptografia

Qualquer um destes registros pode vir precedido de uma mensagem especial. A listagem completa de todas as possíveis mensagens especiais e seus significados se encontra no apêndice A.

- **Protocolo TCP**

Formato do registro:

```
<Data> <Hora> - <Repetição> <Ação> TCP <Status> <IP origem> <Porta
origem> <IP destino> <Porta destino> <Flags> <Interface>
```

Descrição dos campos:

Data: Data em que o registro foi gerado.
Hora: Hora em que o registro foi gerado.
Repetição: Número de vezes em que o registro se repetiu seguidamente. Este campo é mostrado entre parênteses na interface texto.
Status: Este campo, que aparece entre parênteses na interface texto, consiste de uma a três letras, independentes, que possuem o significado abaixo:

A: Pacote autenticado
E: Pacote encriptado
S: Pacote usando troca de chaves via SKIP ou AKER-CDP

Ação: Este campo indica qual foi a ação tomada pelo firewall com relação ao pacote. Ele pode assumir os seguintes valores:

A: Indica que o pacote foi aceito pelo firewall
D: Indica que o pacote foi descardado
R: Indica que o pacote foi rejeitado

IP origem: Endereço IP de origem do pacote que gerou o registro.
Porta origem: Porta de origem do pacote que gerou o registro.
IP destino: Endereço IP destino do pacote que gerou o registro.
Porta destino: Porta destino do pacote que gerou o registro.
Flags: Flags do protocolo TCP presentes no pacote que gerou o registro. Este campo consiste de uma a seis letras independentes. A presença de uma letra, indica que o flag correspondente a ela estava presente no pacote. O significado das letras é o seguinte:

S: SYN
F: FIN
A: ACK

P: PUSH
R: RST (Reset)
U: URG (Urgent Pointer)

Interface: Interface de rede do firewall por onde o pacote foi recebido.

- **Protocolo UDP**

Formato do registro:

```
<Data> <Hora> - <Repetição> <Ação> UDP <Status> <IP origem> <Porta
origem> <IP destino> <Porta destino> <Interface>
```

Descrição dos campos:

Data: Data em que o registro foi gerado.
Hora: Hora em que o registro foi gerado.
Repetição: Número de vezes em que o registro se repetiu seguidamente. Este campo é mostrado entre parênteses na interface texto.
Status: Este campo, que aparece entre parênteses na interface texto, consiste de uma a três letras, independentes, que possuem o significado abaixo:

A: Pacote autenticado
E: Pacote encriptado
S: Pacote usando troca de chaves via SKIP ou AKER-CDP

Ação: Este campo indica qual foi a ação tomada pelo firewall com relação ao pacote. Ele pode assumir os seguintes valores:

A: Indica que o pacote foi aceito pelo firewall
D: Indica que o pacote foi descartado
R: Indica que o pacote foi rejeitado

IP origem: Endereço IP de origem do pacote que gerou o registro.
Porta origem: Porta de origem do pacote que gerou o registro.
IP destino: Endereço IP destino do pacote que gerou o registro.
Porta destino: Porta destino do pacote que gerou o registro.
Interface: Interface de rede do firewall por onde o pacote foi recebido.

- **Protocolo ICMP**

Formato do registro:

```
<Data> <Hora> - <Repetição> <Ação> ICMP <Status> <IP origem> <IP
destino> <Tipo de serviço> <Interface>
```

Descrição dos campos:

Data: Data em que o registro foi gerado.
Hora: Hora em que o registro foi gerado.
Repetição: Número de vezes em que o registro se repetiu seguidamente. Este campo é

mostrado entre parênteses na interface texto.
Status: Este campo, que aparece entre parênteses na interface texto, consiste de uma a três letras, independentes, que possuem o significado abaixo:

A: Pacote autenticado
E: Pacote encriptado
S: Pacote usando troca de chaves via SKIP ou AKER-CDP

Ação: Este campo indica qual foi a ação tomada pelo firewall com relação ao pacote. Ele pode assumir os seguintes valores:

A: Indica que o pacote foi aceito pelo firewall
D: Indica que o pacote foi descartado
R: Indica que o pacote foi rejeitado

IP origem: Endereço IP de origem do pacote que gerou o registro.
IP destino: Endereço IP destino do pacote que gerou o registro.
Tipo de serviço: Tipo de serviço ICMP do pacote que gerou o registro.
Interface: Interface de rede do firewall por onde o pacote foi recebido.

- **Outros procotolos**

Formato do registro:

```
<Data> <Hora> - <Repetição> <Ação> <Protocolo> <Status> <IP origem>
<IP destino> <Interface>
```

Descrição dos campos:

Data: Data em que o registro foi gerado.
Hora: Hora em que o registro foi gerado.
Repetição: Número de vezes em que o registro se repetiu seguidamente. Este campo é mostrado entre parênteses na interface texto.
Status: Este campo, que aparece entre parênteses na interface texto, consiste de uma a três letras, independentes, que possuem o significado abaixo:

A: Pacote autenticado
E: Pacote encriptado
S: Pacote usando troca de chaves via SKIP ou AKER-CDP

Ação: Este campo indica qual foi a ação tomada pelo firewall com relação ao pacote. Ele pode assumir os seguintes valores:

A: Indica que o pacote foi aceito pelo firewall
D: Indica que o pacote foi descardado
R: Indica que o pacote foi rejeitado

Protocolo: Nome do protocolo do pacote que gerou o registro (caso o firewall não consiga resolver o nome do protocolo, será mostrado o seu número)**.**
IP origem: Endereço IP de origem do pacote que gerou o registro.

IP destino: Endereço IP destino do pacote que gerou o registro.
Interface: Interface de rede do firewall por onde o pacote foi recebido.

Registros gerados pelo conversor de endereços

Formato do registro:

```
<Data> <Hora> - <Repetição> C <Protocolo> <IP origem> <Porta origem>
<IP convertido> <Porta convertida>
```

Descrição dos campos dos registros

Data: Data em que o registro foi gerado.
Hora: Hora em que o registro foi gerado.
Repetição: Número de vezes que o registro se repetiu seguidamente. Este campo é mostrado entre parênteses na interface texto.
Protocolo: É o protocolo do pacote que gerou o registro. Pode ser TCP ou UDP.
IP origem: Endereço IP de origem do pacote que gerou o registro.
Porta origem: Porta de origem do pacote que gerou o registro.
IP convertido: Endereço IP para o qual o endereço de origem do pacote foi convertido.
Porta convertida: Porta para qual a porta de origem do pacote foi convertida.

14-3 Utilizando a interface texto

A interface texto para o acesso ao log tem funcionalidade similar à da interface gráfica, porém possui opções de filtragem bem mais limitadas. Além disso, através da interface texto, não se tem acesso às informações complementares que são mostradas quando se seleciona uma entrada do log na interface gráfica ou quando se ativa a opção *Expande mensagens*.

Localização do programa: `/etc/firewall/fwlog`

Sintaxe:

```
Firewall Aker - Versao 5.1
fwlog apaga [log | eventos] [<data_inicio> <data_fim>]
fwlog mostra [log | eventos] [local | cluster] [<data_inicio>
<data_fim>] [prioridade]
```

Ajuda do programa:

```
Uso: fwlog ajuda
     fwlog apaga [log | eventos] [<data_inicio> <data_fim>]
     fwlog mostra [log | eventos] [local | cluster] [<data_inicio>
<data_fim>] [prioridade]

fwlog - Interface texto para visualizar log e eventos
     mostra   = lista o conteudo do log ou dos eventos. Ele pode
mostra
                apenas o log local ou todo o log do cluster
     apaga    = apaga todos os registro do log ou dos eventos
     ajuda    = mostra esta mensagem
Para mostra temos:
```

```
     data_inicio = data a partir da qual os registros serao mostrados
     data_fim    = data ate onde mostrar os registros
                   (As datas devem estar no formato dd/mm/aaaa
                  (Se nao forem informadas as datas, mostra os
registros de
                   hoje)
     prioridade  = campo opcional. Se for informado deve ter um dos
seguintes
                   valores: ERRO, ADVERTENCIA, NOTICIA, INFORMACAO ou
DEPURACAO
                   (Ao selecionar uma prioridade, somente serao
listados
                    registros cuja prioridade for igual a informada)
```

Exemplo 1: (mostrando o log do dia 07/07/2003)

```
#fwlog mostra log 07/07/2003 07/07/2003

07/07/2003 19:06:54 (01) D UDP 10.4.1.126 137 10.4.1.255 137 de0
07/07/2003 19:06:47 (01) D UDP 10.4.1.120 138 10.4.1.255 138 de0
07/07/2003 19:06:35 (01) D UDP 10.4.1.210 138 10.4.1.255 138 de0
07/07/2003 19:06:22 (01) A TCP 10.4.1.24 1027 10.5.1.1 23 de0
07/07/2003 19:06:21 (02) R TCP 10.4.1.2 1028 10.7.1.14 79 de0
07/07/2003 19:06:21 (01) A ICMP 10.5.1.134 10.4.1.12 8 de1
07/07/2003 19:06:20 (01) A ICMP 10.4.1.12 137 10.5.1.134 0 de0
07/07/2003 19:06:02 (01) A UDP 10.4.1.59 1050 10.7.1.25 53 de0
```

Exemplo 2: (mostrando o log do dia 07/07/2003, apenas prioridade notícia)

```
#fwlog mostra log 07/07/2003 07/07/2003 noticia

07/07/2003 19:06:54 (01) D UDP 10.4.1.126 137 10.4.1.255 137 de0
07/07/2003 19:06:47 (01) D UDP 10.4.1.120 138 10.4.1.255 138 de0
07/07/2003 19:06:35 (01) D UDP 10.4.1.210 138 10.4.1.255 138 de0
07/07/2003 19:06:21 (02) R TCP 10.4.1.2 1028 10.7.1.14 79 de0
```

Exemplo 3: (apagando o arquivo de log)

```
#fwlog apaga log 21/10/2003 23/10/2003
Remocao dos registros foi solicitada ao servidor de log
```

15-0 Visualizando os Eventos do Sistema

Neste capítulo mostraremos como visualizar os eventos do sistema, um recurso muito útil para se acompanhar o funcionamento do firewall e detectar possíveis ataques e erros de configuração

O que são os eventos do sistema ?

Eventos são as mensagens do firewall de nível mais alto, ou seja, não relacionadas diretamente a pacotes (como é o caso do log). Nos eventos, podem aparecer mensagens geradas por qualquer um dos três grandes módulos (filtro de pacotes, conversor de endereços e autenticação/criptografia) e por qualquer outro componente do firewall, como por exemplo os proxies e os processos servidores encarregados de tarefas específicas.

Basicamente, o tipo de informação mostrada varia desde mensagens úteis para se acompanhar o funcionamento do sistema (uma mensagem gerada todas as vezes que a máquina é reinicializada, todas as vezes que alguém estabelece uma sessão com o firewall, etc) até mensagens provocadas por erros de configuração ou de execução.

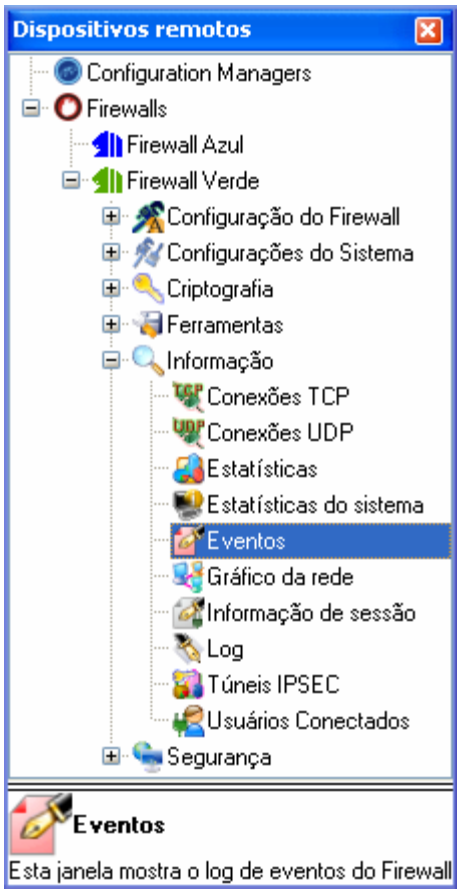
O que é um filtro de eventos ?

Mesmo que o sistema tenha sido configurado para registrar todos os possíveis eventos, muitas vezes se está interessado em alguma informação específica (por exemplo, suponha que se deseje ver todas as mensagens do dia de ontem). O filtro de eventos é um mecanismo oferecido pelo Firewall Aker para se criar visões do conjunto total de mensagens, possibilitando que se obtenha as informações desejadas facilmente.

O filtro só permite a visualização de informações que tiverem sido registradas nos eventos. Caso se deseje obter uma determinada informação, é necessário inicialmente configurar o sistema para registrá-la e então utilizar um filtro para visualizá-la.

15-1 Utilizando a interface gráfica

Para ter acesso a janela de eventos basta:



- Clicar no menu *Informação* do firewall que se deseja visualizar os eventos
- Selecionar a opção *Eventos*

A barra de ferramentas de Eventos

Todas as vezes que se seleciona a opção *Eventos*, é mostrada automaticamente a barra de ferramentas de Eventos. Esta barra, que estará ao lado das outras barras, poderá ser arrastada e ficar flutuando acima das informações dos Eventos. Ela tem o seguinte formato:

Significado dos Ícones:

Abre a janela de filtragem do firewall

Este ícone somente irá aparecer quando o firewall estiver fazendo uma procura nos Eventos. Ele permite interromper a busca do firewall

Exporta os Eventos para diversos formatos de arquivos

Apaga os Eventos do firewall

Permite fazer uma atualização da tela de logs dentro de um determinado período definido no campo seguinte

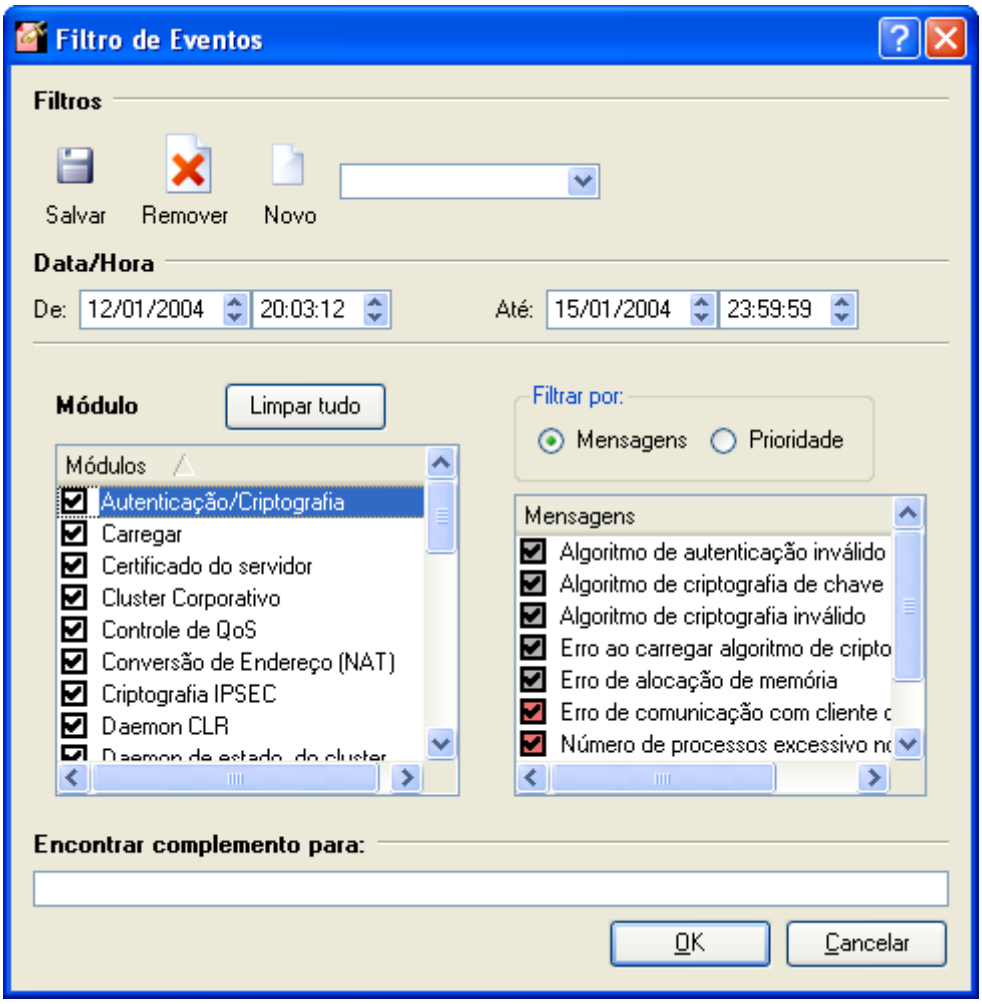
Define o tempo que o firewall irá atualizar a janela com informações de log

Percorre os Eventos para frente e para trás

Expande as mensagens de Eventos, mostrando as mesmas com o máximo de informação

Ao clicar no ícone de filtragem a seguinte janela será mostrada:

A janela de filtro de eventos



Na parte superior da janela, encontram-se os botões **Salvar**, **Remover e Novo**. O botão Salvar permite que se salve os campos de um filtro de forma a facilitar sua aplicação posterior e o botão excluir permite que se exclua um filtro salvo não mais desejado.

Para salvar um filtro de eventos, deve-se proceder da seguinte forma:

1. Preenche-se todos os seus campos da forma desejada.
2. Define-se, no campo **Filtros**, o nome pelo qual ele será referenciado.
3. Clica-se no botão Salvar.

Para se aplicar um filtro salvo, basta selecionar seu nome no campo **Filtros** e todos os campos serão automaticamente preenchidos com os dados salvos.

Para excluir um filtro que não mais seja desejado, deve-se proceder da seguinte forma:

1. Seleciona-se o filtro a ser removido, no campo **Filtros**.
2. Clica-se no botão Excluir.

O filtro padrão é configurado para mostrar todos as mensagens do dia atual. Para se alterar a visualização para outros dias, pode-se configurar a **Data Inicial** e a **Data Final** para os dias desejados (a faixa de visualização compreende os registros da data inicial à data final, inclusive).

Além de se especificar as datas, é possível também se determinar quais mensagens devem ser mostradas. A opção **Filtrar por** permite se escolher entre a listagem de mensagens ou de prioridades.

- **Filtragem por mensagens**

Ao se selecionar filtragem por mensagens, será mostrado na lista do lado esquerdo da janela o nome de todos os módulos que compõem o firewall. Ao se clicar em um destes módulos, será mostrada na lista à direita as diferentes mensagens que podem ser geradas por ele.

Dica: Para se selecionar todas as mensagens de um modulo, basta se clicar sobre a caixa à esquerda do nome do módulo.

- **Filtragem por prioridade**

Diferentes tipos de mensagens possuem prioridades diferentes. Quanto maior for a prioridade associada a um determinado registro, mais importância deve-se dar a ele.

Ao se selecionar filtragem por prioridade, será mostrado na lista do lado esquerdo da janela o nome de todos os módulos que compõem o firewall. Ao se clicar em um destes módulos, será mostrada na lista à direita as diferentes prioridades das mensagens que podem ser geradas por ele.

Abaixo está a lista com as todas as prioridades possíveis, ordenada da mais importante para a menos (caso tenha se configurado o firewall para mandar uma cópia dos eventos para o syslogd, as prioridades com as quais as mensagens serão geradas no syslog são as mesmas apresentadas abaixo):

- Erro

Os registros que se enquadram nesta prioridade indicam algum tipo de erro de configuração ou de operação do sistema (por exemplo, falta de memória). Mensagens desta prioridade são raras e devem ser tratadas imediatamente.

- Alerta

Os registros que se enquadrarem nesta prioridade indicam que algum tipo de situação séria e não considerada normal ocorreu (por exemplo, uma falha na validação de um usuário ao estabelecer uma sessão de administração remota).

- Aviso

Se enquadram nesta prioridade registros que trazem informações que são consideradas importantes para o administrador do sistema, mas estão associadas a uma situação normal (por exemplo, um administrador iniciou uma sessão remota de administração).

- Informação

Os registros desta prioridade acrescentam informações úteis mas não tão importantes para a administração do Firewall (por exemplo, uma sessão de administração remota foi finalizada).

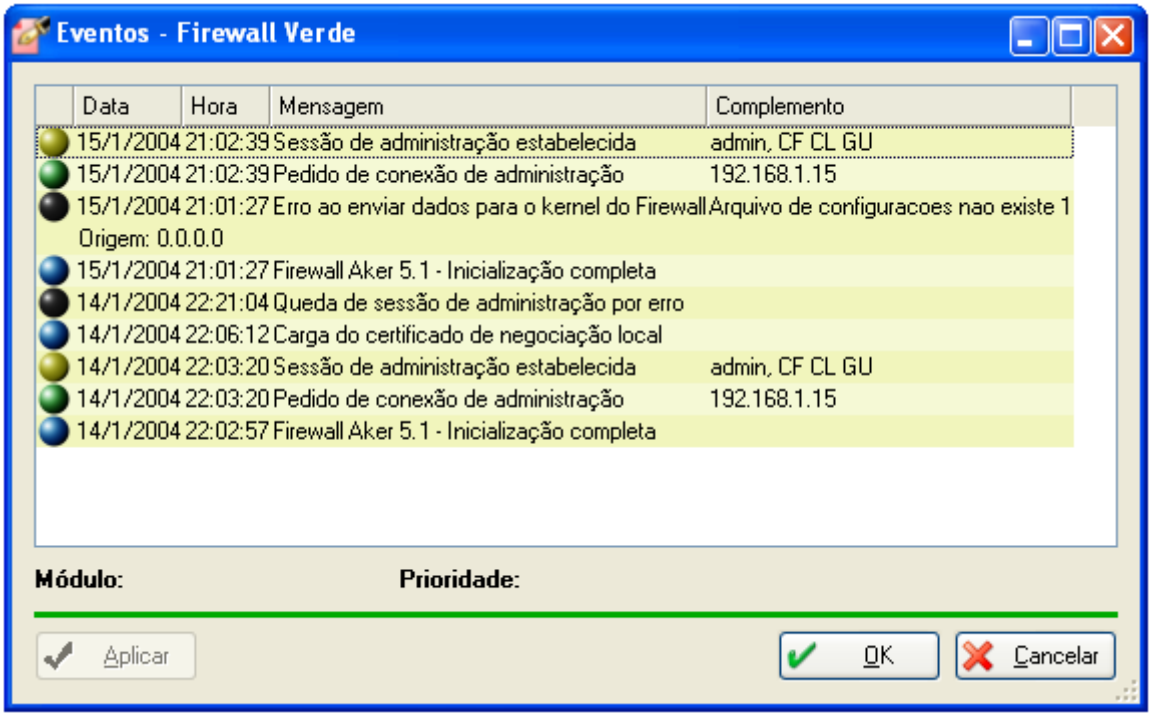
- Depuração

Os registros desta prioridade não trazem nenhuma informação realmente importante, exceto no caso de uma auditoria. Nesta prioridade se encaixam as mensagens geradas pelo módulo de administração remota todas as vezes que é feita uma alteração na configuração do firewall e uma mensagem gerada todas as vezes que o firewall é reinicializado.

Como última opção de filtragem, existe o campo **Filtrar no complemento por**. Este campo permite que se especifique um texto que deve existir nos complementos de todas as mensagens para que elas sejam mostradas. Desta forma, é possível, por exemplo, se visualizar todas as páginas WWW acessadas por um determinado usuário, bastando para isso que se coloque seu nome neste campo.

- O botão **OK** aplicará o filtro escolhido e mostrará a janela de eventos, com as informações selecionadas.
- O botão **Cancelar** fará com que a operação de filtragem seja cancelada e a janela de eventos será mostrada com as informações anteriores.

A janela de eventos


Eventos - Firewall Verde
Data
Hora
Mensagem
Complemento
15/1/2004 21:02:39 Sessão de administração estabelecida admin, CF CL GU
15/1/2004 21:02:39 Pedido de conexão de administração 192.168.1.15
15/1/2004 21:01:27 Erro ao enviar dados para o kernel do Firewall Arquivo de configuracoes nao existe 1
Origem: 0.0.0.0
15/1/2004 21:01:27 Firewall Aker 5.1 - Inicialização completa
14/1/2004 22:21:04 Queda de sessão de administração por erro
14/1/2004 22:06:12 Carga do certificado de negociação local
14/1/2004 22:03:20 Sessão de administração estabelecida admin, CF CL GU
14/1/2004 22:03:20 Pedido de conexão de administração 192.168.1.15
14/1/2004 22:02:57 Firewall Aker 5.1 - Inicialização completa
Módulo:
Prioridade:
Aplicar
OK
Cancelar

A janela de eventos será mostrada após a aplicação de um filtro novo. Ela consiste de uma lista com várias mensagens. Normalmente, cada linha corresponde a uma mensagem distinta, porém existem mensagens que podem ocupar 2 ou 3 linhas. O formato das mensagens será mostrado na próxima seção.

Observações importantes:

- As mensagens serão mostradas de 100 em 100.
- Só serão mostradas as primeiras 10.000 mensagens que se enquadrem no filtro escolhido. As demais podem ser vistas exportando os eventos para um arquivo ou utilizando um filtro que produza um número menor de mensagens.
- No lado esquerdo de cada mensagem, será mostrado um ícone colorido simbolizando sua prioridade. As cores tem o seguinte significado:

Azul	Depuração
Verde	Informação
Amarelo	Notícia
Vermelho	Advertência
Preto	Erro

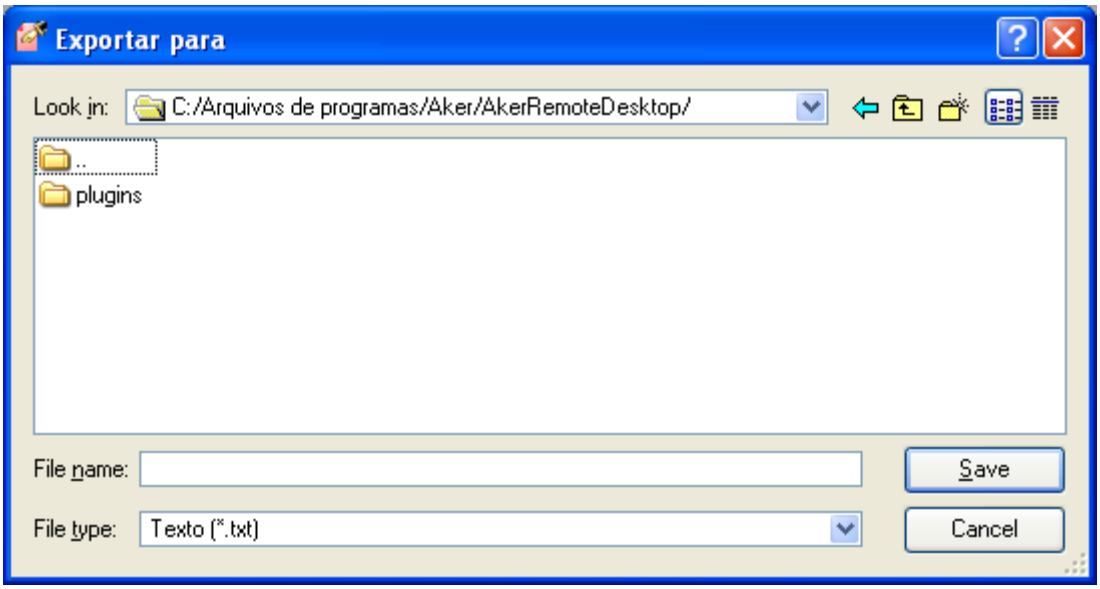
- Ao se clicar com o botão esquerdo sobre uma mensagem, aparecerá na parte inferior da tela uma linha com informações adicionais sobre ela.

Ao se apagar todos os eventos, não existe nenhuma maneira de se recuperar as informações anteriores. A única possibilidade de recuperação é a restauração de uma cópia de segurança.

- O botão **Salvar**, localizado na barra de ferramentas, gravará todas as informações selecionadas pelo filtro atual em um arquivo em formato texto ou em formatos que permitem sua importação pelos analisadores de log da Aker e da WebTrends(R). Os arquivos consistirão de várias linhas de conteúdo igual ao mostrado na janela.

Se a opção *Expande mensagens* estiver marcada e se tiver escolhido a opção de exportação em formato texto, os eventos serão exportados com as mensagens complementares; caso contrário, os eventos serão exportados sem elas.

Esta opção é bastante útil para se enviar uma cópia do log para alguma outra pessoa, para se guardar uma cópia em formato texto de informações importantes ou para se importar os eventos por um analisadores de log citados acima. Ao ser clicado, será mostrada a seguinte janela:



Para exportar o conteúdo dos eventos, basta fornecer o nome do arquivo a ser criado, escolher seu formato e clicar no botão **Salvar**. Para cancelar a operação, clique em **Cancelar**.

Se já existir um arquivo com o nome informado ele será apagado.

- O botão **Próximos 100**, representado como uma seta para a direita na barra de ferramentas, mostrará as últimas 100 mensagens selecionadas pelo filtro. Se não existirem mais mensagens, esta opção estará desabilitada.
- O botão **Últimos 100**, representado como uma seta para a esquerda na barra de ferramentas, mostrará as 100 mensagens anteriores. Se não existirem mensagens anteriores, esta opção estará desabilitada.
- O botão **Ajuda** mostrará a janela de ajuda específica para a janela de eventos.

15-2 Formato e significado dos campos das mensagens de eventos

Abaixo segue a descrição do formato das mensagens, seguido de uma descrição de cada um de seus campos. A listagem completa de todas as possíveis mensagens e seus significados se encontra no apêndice A.

Formato do registro:

```
<Data> <Hora> <Mensagem> [Complemento]
[Mensagem complementar 1]
[Mensagem complementar 2]
```

Descrição dos campos:

Data: Data em que o registro foi gerado.
Hora: Hora em que o registro foi gerado.
Mensagem: Mensagem textual que relata o acontecimento
Complemento: Este campo traz informações complementares e pode ou não aparecer,

dependendo da mensagem. Na interface texto, caso ele apareça, virá entre parênteses. **Mensagem complementar 1 e 2:** Estes complementos só existem no caso de mensagens relacionadas à conexões tratadas pelos proxies transparentes e não-transparentes e são mostrados sempre na linha abaixo da mensagem a que se referem. Nestas mensagens complementares, se encontram o endereço origem da conexão e, no caso dos proxies transparentes, o endereço destino.

15-3 Utilizando a interface texto

A interface texto para o acesso aos eventos tem funcionalidade similar à da interface gráfica. Todas as funções da interface gráfica estão disponíveis, exceto a opção de filtragem de mensagens e o fato de que através da interface texto não se tem acesso às informações complementares que são mostradas quando se seleciona uma mensagem de eventos na interface gráfica ou quando se ativa a opção *Expande mensagens*.

O programa que faz a interface texto com os eventos é o mesmo usado para a interface com o log e foi mostrado também no capítulo anterior.

Localização do programa: `/etc/firewall/fwlog`

Sintaxe:

```
Firewall Aker - Versao 5.1
fwlog apaga [log | eventos] [<data_inicio> <data_fim>]
fwlog mostra [log | eventos] [local | cluster] [<data_inicio>
<data_fim>] [prioridade]
```

Ajuda do programa:

```
Uso: fwlog ajuda
     fwlog apaga [log | eventos] [<data_inicio> <data_fim>]
     fwlog mostra [log | eventos] [local | cluster] [<data_inicio>
<data_fim>] [prioridade]

fwlog - Interface texto para visualizar log e eventos
     mostra   = lista o conteudo do log ou dos eventos. Ele pode
mostra
                apenas o log local ou todo o log do cluster
     apaga    = apaga todos os registro do log ou dos eventos
     ajuda    = mostra esta mensagem
Para mostra temos:
     data_inicio = data a partir da qual os registros serao mostrados
     data_fim    = data ate onde mostrar os registros
                   (As datas devem estar no formato dd/mm/aaaa
                  (Se nao forem informadas as datas, mostra os
registros de
                   hoje)
     prioridade  = campo opcional. Se for informado deve ter um dos
seguintes
                   valores: ERRO, ADVERTENCIA, NOTICIA, INFORMACAO ou
DEPURACAO
                   (Ao selecionar uma prioridade, somente serão
listados
                    registros cuja prioridade for igual a informada)
```

Exemplo 1: (mostrando os eventos do dia 07/10/2003 ao dia 08/10/2003)

```
#fwlog mostra eventos 07/10/2003 08/10/2003

08/10/2003 11:39:35 Sessao de administracao finalizada
08/10/2003 09:13:09 Sessao de administracao estabelecida
(administrador, CF CL GU)
08/10/2003 09:13:09 Pedido de conexao de administracao (10.4.1.14)
08/10/2003 09:09:49 Operacao sobre o arquivo de log (Compactar)
07/10/2003 10:27:11 Aker Firewall v5.1 - Inicializacao completa
07/10/2003 08:57:11 Tabela de conversão UDP cheia
```

Exemplo 2: (mostrando os eventos do dia 07/10/2003 ao dia 08/10/2003, apenas prioridade depuração)

```
#fwlog mostra eventos 07/10/2003 08/10/2003 depuracao

08/10/2003 09:09:49 Operacao sobre o arquivo de log (Compactar)
07/10/2003 10:27:11 Aker Firewall v5.1 - Inicializacao completa
```

Exemplo 3: (removendo todo o conteúdo do arquivo de eventos)

```
#fwlog apaga eventos 21/10/2003 23/10/2003

Remocao dos registros foi solicitada ao servidor de log
```

16-0 Visualizando estatísticas

Neste capítulo falaremos do que é, bem como as características da janela de estatística.

O que é a janela de estatísticas do Firewall Aker?

No Firewall, as estatísticas são um método de se medir o tráfego de dados através de suas interfaces. Este tráfego se traduz em números que mostram a quantidade de pacotes enviados ou recebidos, além do tamanho total de bytes trafegados.

Utilizando-se destas informações, o administrador consegue verificar o fluxo de dados de seus serviços podendo, assim saber se o ambiente físico da rede precisa ser melhorado ou expandido.

Outra utilização para este tipo de informação é a realização de bilhetagem da rede. Tendo-se conhecimento da quantidade de bytes que cada máquina transferiu na rede, calcula-se o quanto que cada uma deve ser taxada.

Para se realizar bilhetagem de rede, deve-se criar uma regra de filtragem com um acumulador diferente para cada máquina a ser taxada. Todos os acumuladores devem ter regras de estatísticas associados a eles. Estas regras são configuradas na janela de visualização de estatística.

Como funcionam as estatísticas do Firewall Aker ?

O fucionamento das estatísticas do Firewall Aker se baseia em três etapas distintas:

- Criação de Acumuladores

Nesta etapa, cadastramos os acumuladores que serão associados a regras de filtragem. Eles servem apenas como totalizadores de uma ou mais regras de filtragem. Para maiores informações sobre a criação de acumuladores e sua associação com regras de filtragem, veja os capítulos Cadastrando Entidades e O Filtro de Estados.

- Criação de regras de estatística

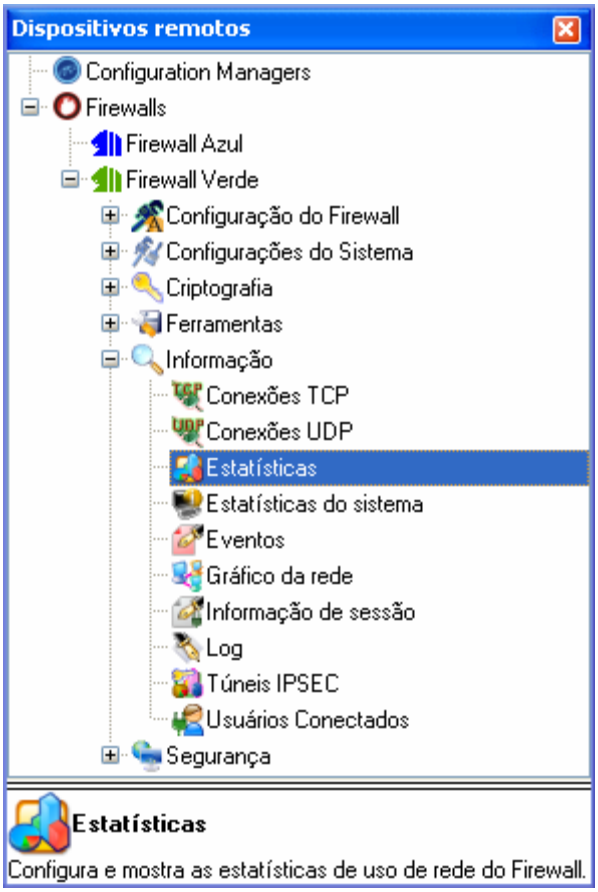
Após a criação dos acumuladores e sua associação com as regras de filtragem desejadas, devemos criar regras de estatística que definem os intervalos de coleta e quais acumuladores serão somados para gerar o valor da estatística em um dado momento. Esta etapa será explicada nesta capítulo.

- Visualização das estatísticas

Após a criação das regras de estatísticas, podemos ver os valores associados a cada uma delas, exportá-los ou traçar gráficos. Esta estapa também será mostrada neste capítulo.

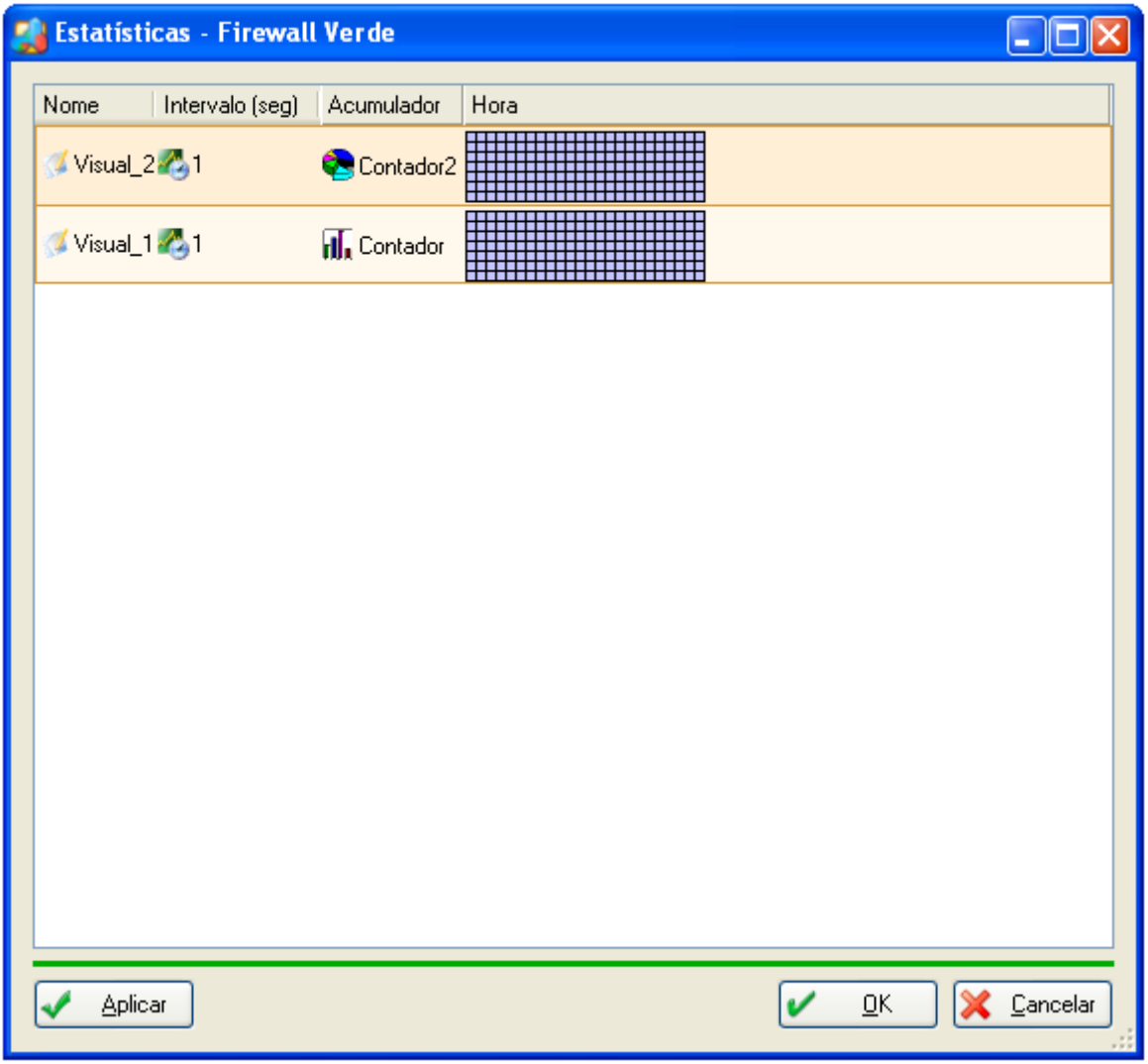
16-1 Utilizando a interface gráfica

Para ter acesso a janela de configuração de estatística basta:



- Clicar no menu *Informação* da janela do firewall que você deseja administrar
- Selecionar o item *Estatísticas*

A janela de regras de estatística



A janela de estatísticas contém todas as regras de estatística definidas no Firewall Aker. Cada regra será mostrada em uma linha separada, composta de diversas células. Caso uma regras esteja selecionada, ela será mostrada em uma cor diferente.

- O botão **OK** fará com que o conjunto de estatísticas seja atualizado e passe a funcionar imediatamente.
- O Botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta
- A barra de rolagem do lado direito serve para visualizar as regras que não couberem na janela.

Cada regra de estatística é composta dos seguintes campos:

- **Nome:** Nome da estatística, utilizada para facilitar a sua referência. Deve possuir um nome único entre o conjunto de regras.
- **Intervalo:** Corresponde ao intervalo de tempo que se fará a totalização da regra, ou seja, a soma dos valores de todos os acumuladores presentes na regra.
- **Acumulador:** Este campo define quais os acumuladores farão parte da regra.

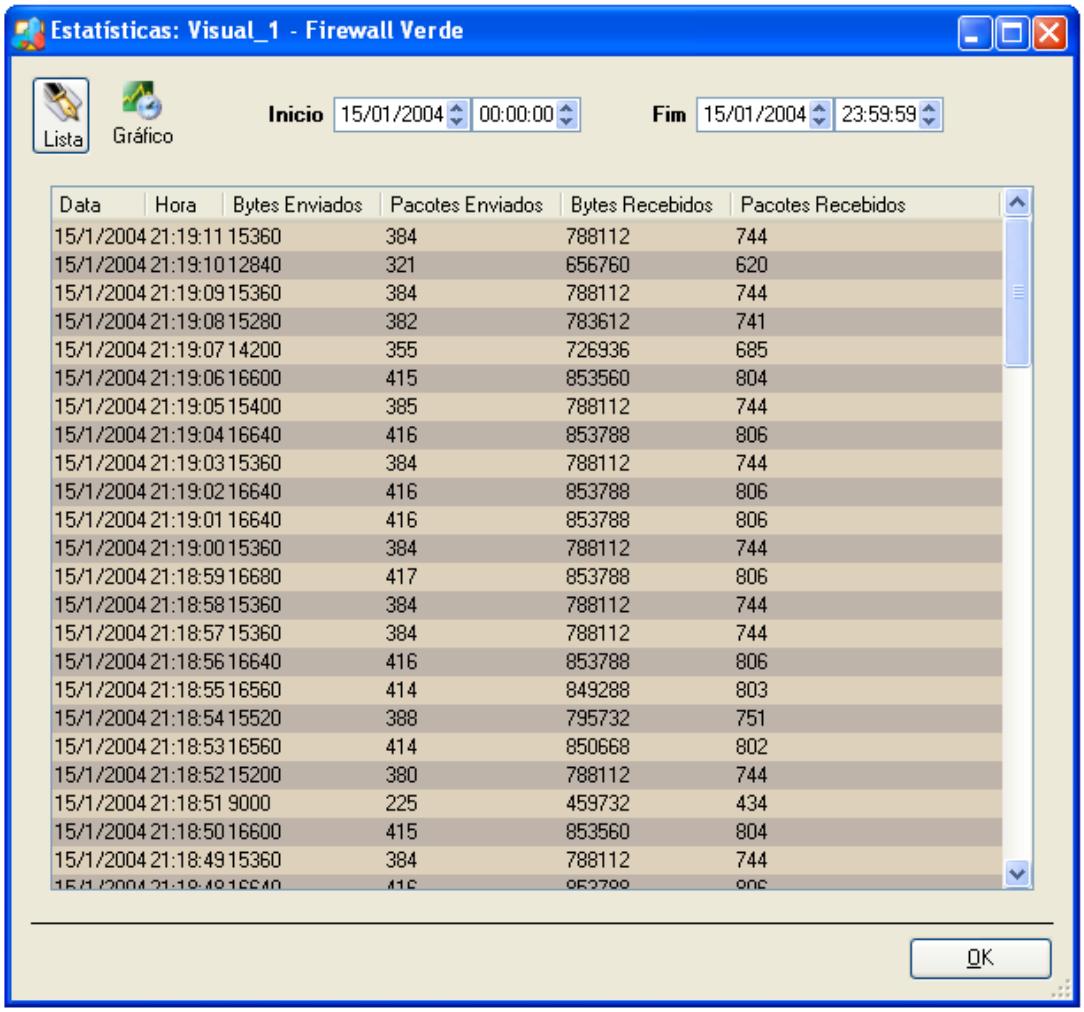
- **Hora:** Esta tabela define as horas e dias da semana em que a regra é aplicável. As linhas representam os dias da semana e as colunas as horas. Caso se queira que a regra seja aplicável em determinada hora o quadrado deve ser preenchido, caso contrário o quadrado deve ser deixado em branco.

Para interagir com a janela de regras, utilize a barra de ferramentas localizada na parte superior da janela ou clicar com o botão direito sobre ela.

- **Inserir:** Esta opção permite se incluir uma nova regra na lista.
- **Apagar**: Esta opção remove da lista a regra selecionada.
- **Copiar:** Esta opção copia a regra selecionada para uma área temporária.
- **Colar:** Esta opção copia a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.
- **Habilitar/Desabilitar:** Esta opção ativa ou desativa a regra selecionada da lista.
- **Visualização:** Mostrará a janela de visualização de estatísticas relativa a regra selecionada.
- **Nome**: Atribui um nome a regra de estatísticas.

Visualizando estatísticas

Ao se clicar no botão **Visualização** ou clicar duas vezes sobre uma regra de estatística, a seguinte janela será mostrada:

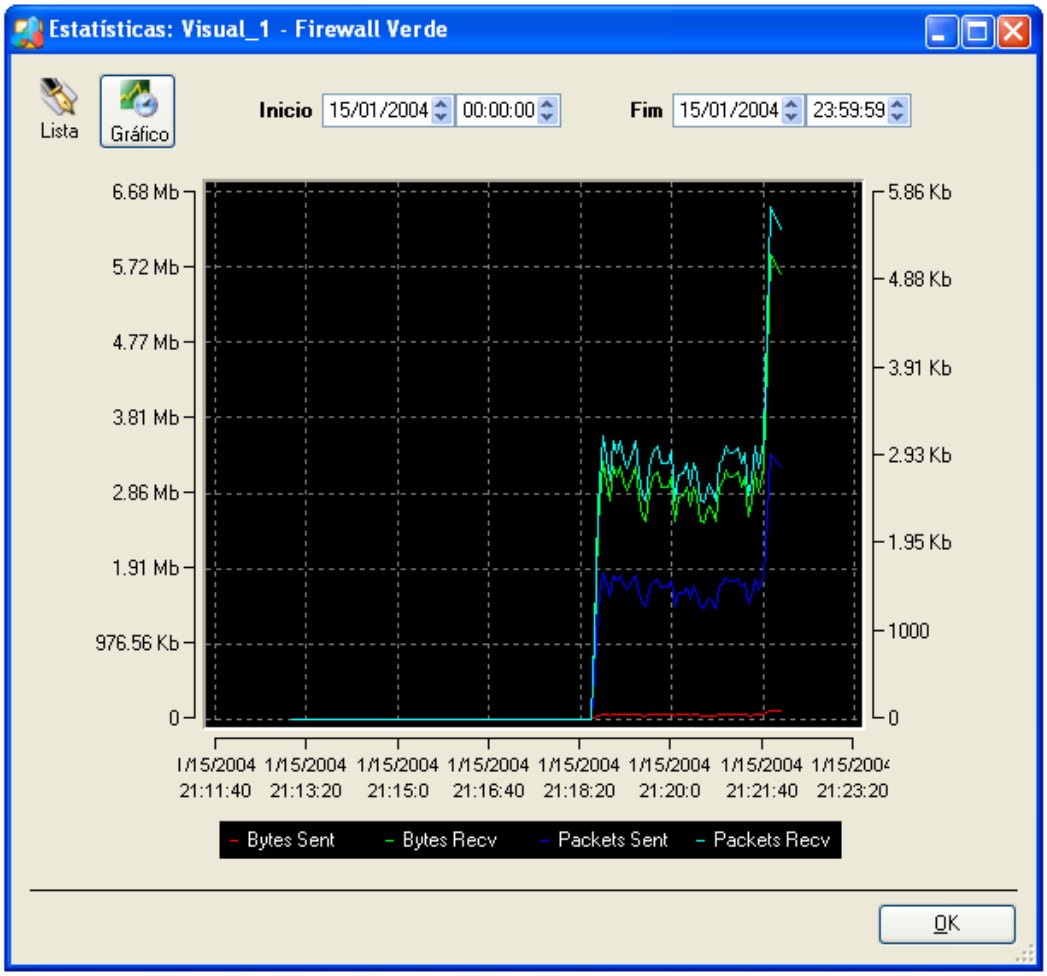


Nesta janela, os dados computados para a estatística selecionada serão mostrados em formato gráfico ou texto. Estas informações são relativas a data de início e fim especificadas na parte superior da janela. Para se alterar esta data deve-se escolher os campos de **Data**, colocando as datas de inicio e de finalização da pesquisa.

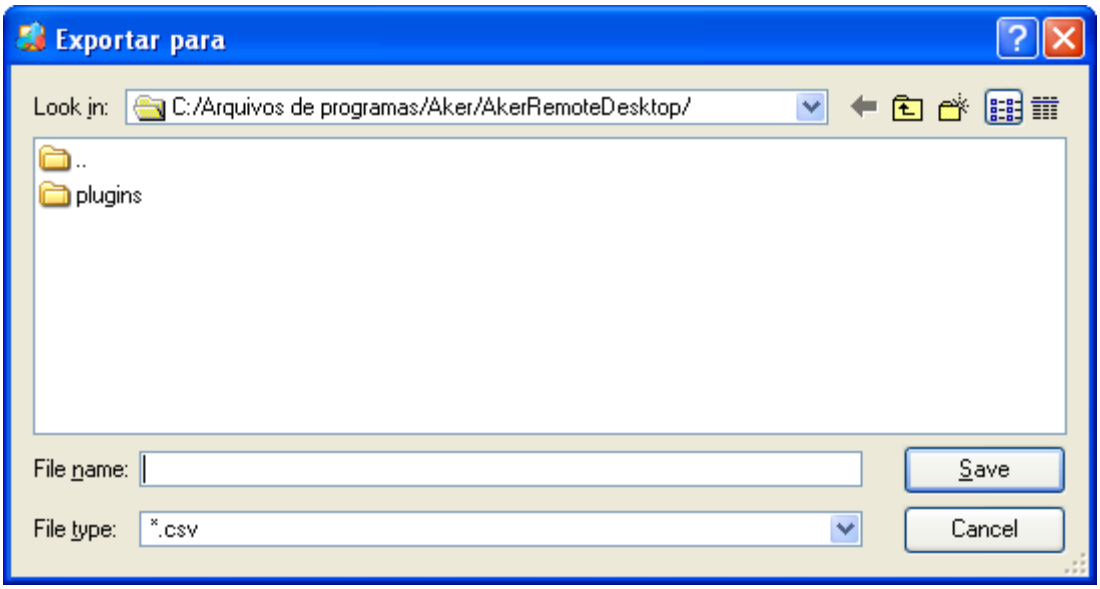
- **Leitura:** Mostra um conjunto de 100 registros de cada vez. Cada registro se refere a contabilização dos acumuladores da estatística em um determinado tempo.

  O botão **Remover** desta pasta irá remover o conjunto de registros com o tempo especificado.

- **Gráfico:** Representa os dados contidos na pasta *Leitura* em formato gráfico. O gráfico é gerado ao ser pressionado o botão na barra de ferramentas. Este gráfico também permite que o usuário selecione qual linha deve ser mostrada pressionando-se os rótulos dos mesmos.



Ao pressionarmos o botão de salvar estatísticas a janela abaixo irá aparecer de modo a se escolher o nome do arquivo. Este arquivo é gravado no formato CSV que permite sua manipulação através de planilhas de cálculo.



A barra de ferramentas da visualização das estatísticas

A barra de ferramentas da visualização das estatísticas terá as seguintes funções:

- O botão salvar registros permite a exportação dos dados gerados pelos contadores.

- Este botão irá excluir os registros selecionados gerados pelos contadores.

- Este é o botão de navegação dos dados registrados pelos contadores e que estão sendo exibidos pelas estatísticas

16-2 Utilizando a interface texto

A interface texto para o acesso às estatísticas tem funcionalidade similar à da interface gráfica. Todas as funções da interface gráfica estão disponíveis, exceto a opção de verificar os dados através de gráfico e de se verificar em quais regras os acumuladores de uma determinada estatística estão presentes.

A tabela de horário é visualizada da seguinte forma:

O símbolo : (dois pontos) informa que a regra é valida para os dois dias da semana que aparecem separados por / .Ex: Dom/Seg
O símbolo . (ponto) informa que a regra so é válida para o dia da semana que segue o caractere / .Ex: Dom/Seg - Seg
O símbolo ' (acento) informa que a regra so é válida para o dia da semana que antecede o caractere / .Ex: Dom/Seg - Dom

Localização do programa: `/etc/firewall/fwstat`

Sintaxe:

```
fwstat ajuda
mostra [[-c] <estatistica> [<data inicial> <data final>]]
inclui <estatistica> <periodo> [<acumulador1> [acumulador2] ...]
remove <estatistica>
desabilita <estatistica> [<dia> <hora>]
habilita <estatistica> [<dia> <hora>]
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
Uso: fwstat ajuda
            mostra [[-c] <estatistica> [<data inicial> <data final>]]
            inclui <estatistica> <periodo> [<acumulador1>
[acumulador2] ...]
            remove <estatistica>
            desabilita <estatistica> [<dia> <hora>]
```

```
            habilita <estatistica> [<dia> <hora>]

     ajuda       = mostra esta mensagem
     mostra      = sem parametros, mostra as estatisticas cadastradas
                   com, mostra os dados coletados para
     estatistica = nome da estatistica
     -c          = resultado no formato CSV (comma separated value)
                   (util para importar dados em planilhas eletronicas)
     datas       = dadas limite para mostrar dados
     inclui      = adiciona uma estatistica de nome "estatistica"
     remove      = remove uma estatistica de nome "estatistica"
     periodo     = periodo de captura dos dados (segundos)
     acumulador_ = nome das entidades acumulador para ler
     desabilita  = desabilita uma estatistica
     habilita    = habilita uma estatistica
     dia, hora   = se especificado (sempre ambos), habilita ou
desabilita
                   apenas para a hora especificada. 'dia' pertence a
                   {dom, seg, ter, ...} e 'hora' a {0..23}
```

Exemplo 1: (mostrando as estatísticas)

```
#fwstat mostra
Nome  : estatistica1                                        (habilitada)
----
Periodo  : 17400 segundo(s)
Acumuladores: a1
Horario  :
Dia\Hora|0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
21 22 23
------------------------------------------------------------------------
---------
Dom/Seg |:  :                          :  :  :  :  :  :  :  :  :  :
:  :  :  :
Ter/Qua |:  :                          :  :  :  :  :  :  :  :  :  :
:  :  :  :
Qui/Sex |:  :                          :  :  :  :  :  :  :  :  :  :
:  :  :  :
Sab     |'  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '
'  '  '  '

Nome  : estatistica2                                        (habilitada)
----
Periodo  : 100  segundo(s)
Acumuladores: a1  a11
Horario  :
Dia\Hora|0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
21 22 23
------------------------------------------------------------------------
---------
Dom/Seg |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
:  :  :  :
Ter/Qua |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
:  :  :  :
Qui/Sex |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
:  :  :  :
Sab     |'  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '
'  '  '  '
```

Exemplo 2: (mostrando a estatística do dia 28/10/2001 ao dia 29/10/2001)

```
#fwstat mostra estatistica 28/10/2001 29/10/2001
Dia        Hora     Enviados (bytes/pacotes)  Recebidos
(bytes/pacotes)
-------------------------------------------------------------------------
-
29/10/2001 17:24:54          320/1                     321/1
29/10/2001 17:23:14          652/6                     654/6
29/10/2001 17:21:34          234/2                     980/9
29/10/2001 17:19:54          324/3                     650/6
29/10/2001 17:18:14          325/3                     150/1
29/10/2001 17:16:34          985/9                     240/2
29/10/2001 17:14:54          842/8                     840/8
29/10/2001 17:13:14          357/3                     289/2
29/10/2001 16:58:14          786/7                     261/2
```

17-0 Visualizando e Removendo Conexões

Neste capítulo mostraremos como visualizar e remover conexões TCP e sessões UDP em tempo real.

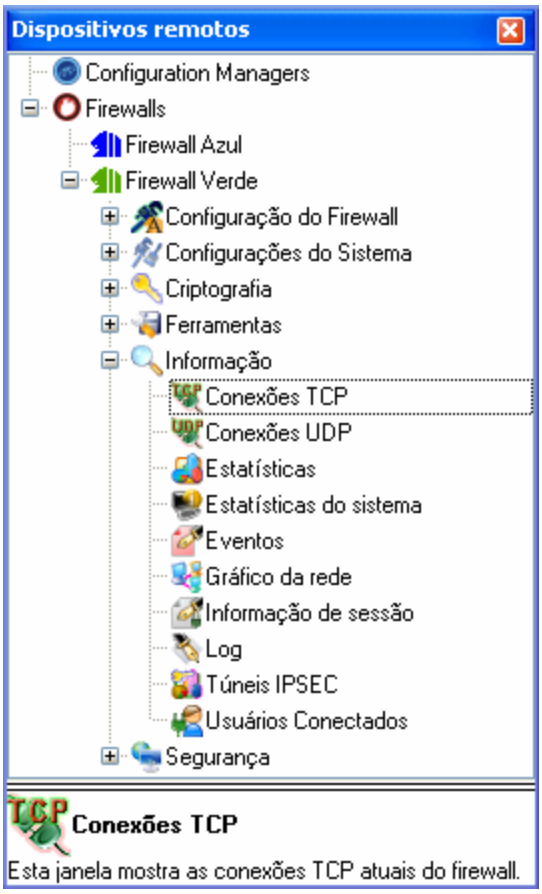
O que são conexões ativas ?

Conexões ativas são conexões TCP ou sessões UDP que estão ativas através do firewall. Cada uma destas conexões foi validada através de uma regra do filtro de estados, acrescentada pelo administrador do sistema, ou por uma entrada na tabela de estados, acrescentada automaticamente pelo Firewall Aker.

Para cada uma destas conexões, o firewall mantém diversas informações em suas tabelas de estado. Algumas destas informações são especialmente úteis para o administrador e podem ser visualizadas a qualquer momento através da janela de conexões ativas. Dentre estas informações, pode-se citar a hora exata do estabelecimento da conexão e o tempo que ela se encontra parada, isto é, sem que nenhum pacote trafegue por ela.

17-1 Utilizando a interface gráfica

Para ter acesso a janela de conexões ativas basta:



- Clicar no menu *Informação* do firewall que se deseja visualizar
- Selecionar *Conexões TCP* ou *Conexões UDP*

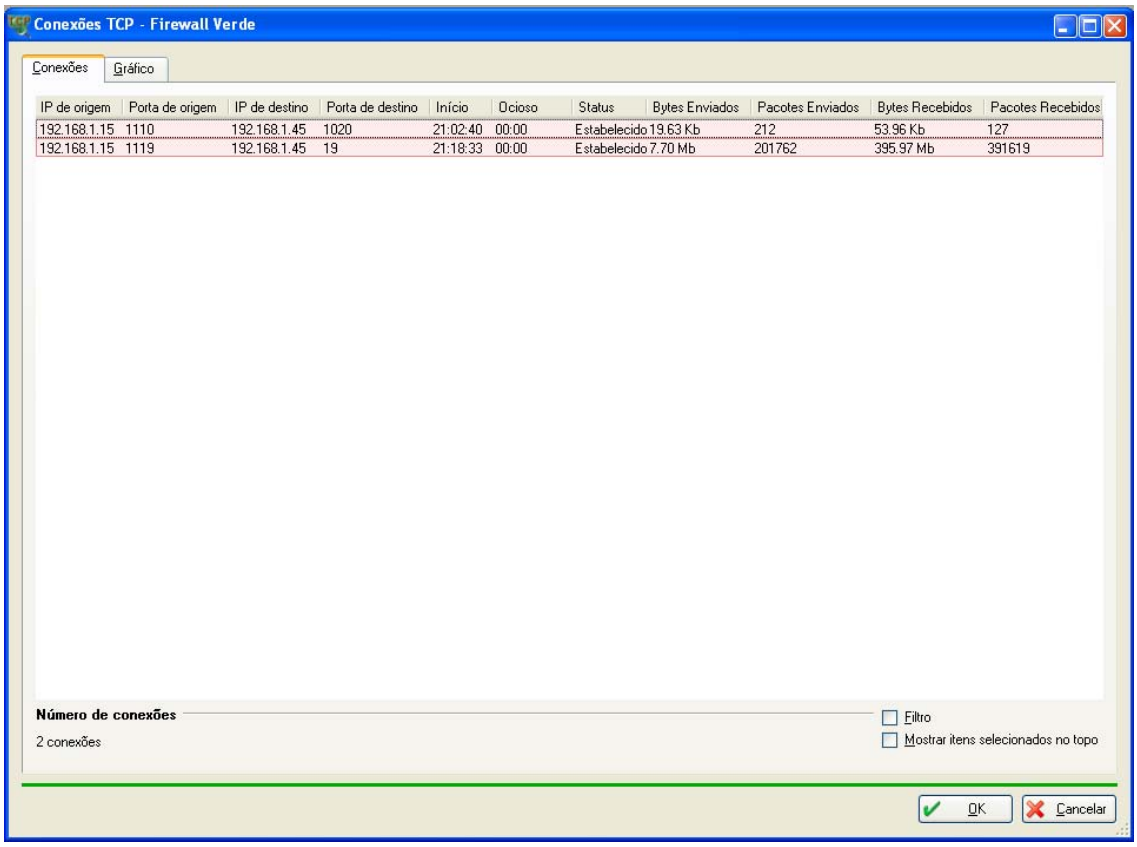
A janela de conexões ativas

A janela de conexões ativas é onde são mostradas todas as conexões que estão passando pelo firewall em um determinado instante. As janelas para os protocolos TCP e UDP são exatamente iguais, com a exceção do campo chamado **Status** que somente existe na janela de conexões TCP.

Para simplificar o entendimento, fala-se de conexões TCP e UDP, entretanto, isto não é totalmente verdadeiro devido ao protocolo UDP ser um protocolo não orientado à conexão. Na verdade, quando se fala em conexões UDP refere-se a sessões onde existe tráfego nos dois sentidos. Cada sessão pode ser vista como o conjunto dos pacotes de requisição e de resposta que fluem através do firewall para um determinado serviço provido por uma determinada máquina e acessado por outra.

Essa janela se compõe de duas pastas: na primeira é mostrada uma lista com as conexões ativas e a segunda fornece um gráfico em tempo real das máquinas e serviços mais acessados.

- **Pasta de conexões**

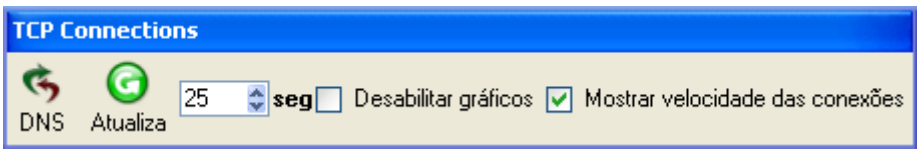

Conexões TCP - Firewall Verde
Conexões
Gráfico
IP de origem | Porta de origem | IP de destino | Porta de destino | Início | Ocioso | Status | Bytes Enviados | Pacotes Enviados | Bytes Recebidos | Pacotes Recebidos
192.168.1.15 1110 192.168.1.45 1020 21:02:40 00:00 Estabelecido 19.63 Kb 212 53.96 Kb 127
192.168.1.15 1119 192.168.1.45 19 21:18:33 00:00 Estabelecido 7.70 Mb 201762 395.97 Mb 391619
Número de conexões
2 conexões
Filtro
Mostrar itens selecionados no topo
OK
Cancelar

Esta pasta consiste de uma lista com uma entrada para cada conexão ativa. Na parte inferior da janela é mostrada uma mensagem informando o número total de conexões ativas em um determinado instante. As velocidades total e média são exibidas na parte inferior da janela.

- O botão **OK** faz com que a janela de conexões ativas seja fechada.
- Caixa **Filtro** exibe as opções de filtragem sendo possível se selecionar os endereços origem ou destino e/ou portas para serem exibidos na janela.
- A opção **Itens selecionados no topo** coloca as conexões selecionadas no topo da janela para melhor visualização.

- A opção **Remover**, que aparece ao se clicar com o botão direito sobre uma conexão, permite que se remova uma conexão.

Ao se remover uma conexão TCP, o firewall envia pacotes de reset para as máquinas participantes da conexão, efetivamente derrubando-a, e remove a entrada de sua tabela de estados. No caso de conexões UDP, o firewall simplesmente remove a entrada de sua tabela de estados, fazendo com que não sejam mais aceitos pacotes para a conexão removida.



- O botão **Atualizar**, localizado na barra de ferramentas faz com que as informações mostradas sejam atualizadas periodicamente de forma automática ou não. Clicando-se sobre ele, alterna-se entre os dois modos de operação. O intervalo de atualização pode ser configurado mudando-se o valor logo à direita deste campo.

- O botão **DNS**, localizado na barra de ferramentas, acionará o serviço de nomes (DNS) para resolver os nomes das máquinas cujos endereços IPs aparecem listados. Cabem ser observados os seguintes pontos:

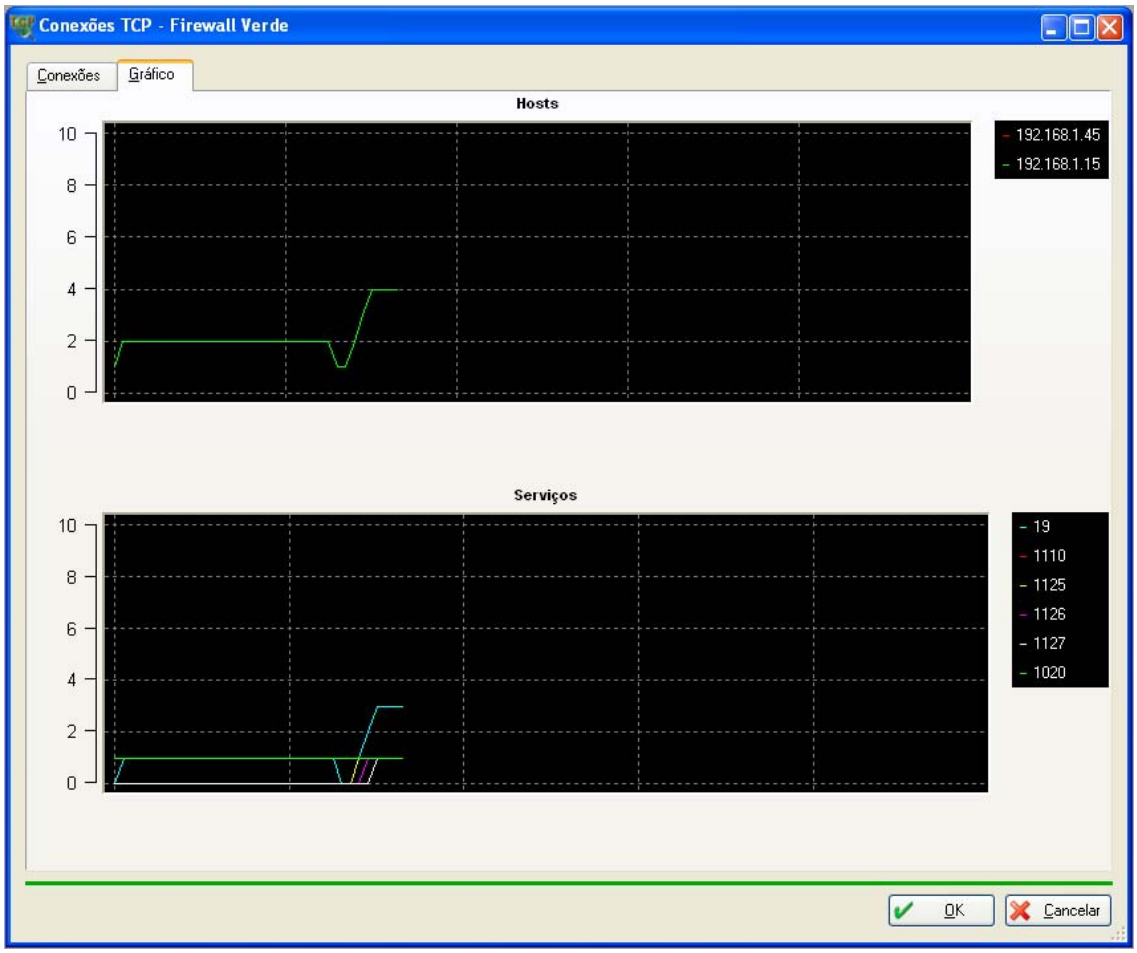
1. A resolução de nomes muitas vezes é um serviço lento e, devido a isso, a tradução dos nomes é feita em segundo plano.
2. Muitas vezes, devido a problemas de configuração do DNS reverso (que é o utilizado para resolver nomes a partir de endereços IP), não será possível a resolução de certos endereços. Neste caso, os endereços não resolvidos serão mantidos na forma original e será indicado ao seu lado que eles não possuem DNS reverso configurado.

- A opção **Desabilitar gráficos** desabilita o desenho do gráfico de conexões, sendo indicada para máquinas especialmente lentas.

- A opção **Mostrar velocidade das conexões**, se ativa, faz com que a interface calcule e mostre a velocidade de cada conexão em bits/s.

- É possível se ordenar a lista das conexões por qualquer um de seus campos, bastanto para isso clicar no título do campo. O primeiro click produzirá uma ordenação ascendente e o segundo uma ordenação descendente.

- **Pasta de gráfico**



Esta pasta consiste de dois gráficos: o gráfico superior mostra os serviços mais utilizados e o gráfico inferior mostra as máquinas que mais acessam serviços ou que mais são acessadas. No lado direito existe uma lengenda mostrando que máquina ou serviço correspondem a que cor do gráfico.

O intervalo de tempo no qual o gráfico é atualizado é o mesmo configurado na pasta de conexões

Significado dos campos de uma conexão ativa

Cada linha presente na lista de conexões ativas representa uma conexão. O significado de seus campos é o seguinte:

IP origem: Endereço IP da máquina que iniciou a conexão.

Porta origem: Porta usada pela máquina de origem para estabelecer a conexão

IP destino: Endereço IP da máquina para a qual a conexão foi efetuada.

Porta destino: Porta para qual a conexão foi estabelecida. Esta porta normalmente está associada a um serviço específico.

Início: Hora de abertura da conexão.

Inativo: Número de minutos e segundos de inatividade da conexão.

Estado Atual: Este campo só aparece no caso de conexões TCP. Ele representa o estado da conexão no instante mostrado e pode assumir um dos seguintes valores:

SYN Enviado: Indica que o pacote de abertura de conexão (pacote com flag de SYN) foi enviado, porém a máquina servidora ainda não respondeu.

SYN Trocados: Indica que o pacote de abertura de conexão foi enviado e a máquina servidora respondeu com a confirmação de conexão em andamento.

Estabelecida: Indica que a conexão está estabelecida.

Escutando Porta: Indica que a máquina servidora está escutando na porta indicada, aguardando uma conexão a partir da máquina cliente. Isto só ocorre no caso de conexões de dados FTP.

Bytes Enviados/Recebidos: Estes campos só aparecem no caso de conexões TCP, e indicam o número de bytes trafegados por esta conexão em cada um dos dois sentidos.

Pacotes Enviados/Recebidos: Estes campos só aparecem no caso de conexões TCP, e indicam o número de pacotes IP trafegados por esta conexão em cada um dos dois sentidos.

17-2 Utilizando a interface texto

A interface texto para acesso à lista de conexões ativas possui as mesmas capacidades da interface gráfica. O mesmo programa trata as conexões TCP e UDP.

Localização do programa: `/etc/firewall/fwlist`

Sintaxe:

```
Uso: fwlist ajuda
     fwlist mostra [[-w] [TCP]] | [UDP] | [sessoes]
     fwlist remove [TCP | UDP] IP_origem Porta_origem IP_destino
Porta_destino
     fwlist remove sessao IP_origem
```

Ajuda do programa:

```
fwlist - Lista e remove conexoes TCP/UDP e sessoes ativas
Uso: fwlist ajuda
     fwlist mostra [[-w] [TCP]] | [UDP] | [sessoes]
     fwlist remove [TCP | UDP] IP_origem Porta_origem IP_destino
Porta_destino
     fwlist remove sessao IP_origem

     ajuda  = mostra esta mensagem
     mostra = lista as conexoes ou sessoes ativas
     remove = remove uma conexao ou sessao ativa
```

Exemplo 1: (listando as conexões ativas TCP)

```
#fwlist mostra TCP

Origem (IP:porta)    Destino (IP:porta)    Inicio   Inativo Estado
-------------------------------------------------------------------
---------
10.4.1.196:1067      10.4.1.11:23          15:35:19 00:00
Estabelecida
10.4.1.212:1078      10.5.2.1:25           15:36:20 00:10
Estabelecida
```

Exemplo 2: (listando as conexões ativas UDP)

```
#fwlist mostra UDP

Origem (IP:porta)    Destino (IP:porta)    Inicio   Inativo
-------------------------------------------------------
10.4.1.1:1099        10.4.1.11:53          15:35:19 00:00
10.4.1.18:1182       10.5.2.1:111          15:36:20 00:10
```

Exemplo 3: (removendo uma conexão TCP e listando as conexões)

```
#fwlist remove tcp 10.4.1.196 1067 10.4.1.11 23

#fwlist mostra TCP

Origem (IP:porta)    Destino (IP:porta)    Inicio   Inativo Estado
-------------------------------------------------------------------
---------
10.4.1.212:1078      10.5.2.1:25           15:36:20 00:10
Estabelecida
```

18-0 Trabalhando com Proxies

Neste capítulo será mostrado toda a base de conhecimento necessária para se entender o funcionamento dos proxies do Firewall Aker. Os detalhes específicos de cada proxy serão mostrados nos próximos capítulos.

18-1 Planejando a instalação

O que são proxies ?

Proxies são programas especializados que geralmente rodam em firewalls e que servem como ponte entre a rede interna de uma organização e os servidores externos. Seu funcionamento é simples: eles ficam esperando por uma requisição da rede interna, repassam esta requisição para o servidor remoto na rede externa, e devolvem sua resposta de volta para o cliente interno.

Na maioria das vezes os proxies são utilizados por todos os clientes de uma sub-rede e devido a sua posição estratégica, normalmente eles implementam um sistema de cache para alguns serviços. Além disso, como os proxies trabalham com dados das aplicações, para cada serviço é necessário um proxy diferente.

Proxies tradicionais

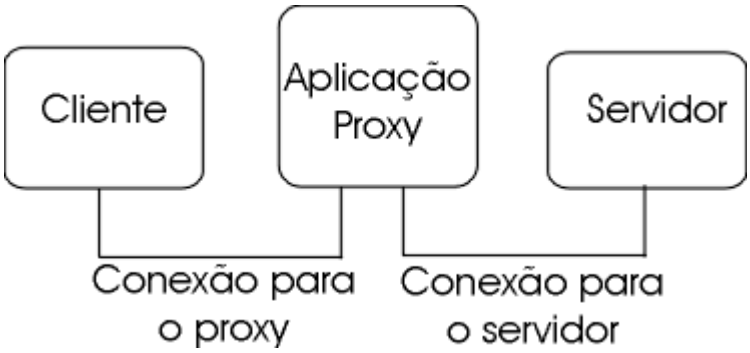
Para que uma máquina cliente possa utilizar os serviços de um proxy, é necessário que a mesma saiba de sua existência, isto é, que ela saiba que ao invés de estabelecer uma conexão com o servidor remoto, ela deve estabelecer a conexão com o proxy e repassar sua solicitação ao mesmo.

Existem alguns clientes que já possuem suporte para proxies embutido neles próprios (como exemplo de clientes deste tipo, pode-se citar a maioria dos browsers existentes atualmente). Neste caso, para se utilizar as funções de proxy, basta-se configurá-los para tal. A grande maioria dos clientes, entretanto, não está preparada para trabalhar desta forma. A única solução possível neste caso, é alterar a pilha TCP/IP em todas as máquinas clientes de modo a fazer com que transparentemente as conexões sejam repassadas para os proxies.

Esta abordagem traz inúmeras dificuldades, já que além de ser extremamente trabalhoso se alterar todas as máquinas clientes, muitas vezes não existe forma de se alterar a implementação TCP/IP de determinadas plataformas, fazendo com que clientes nestas plataformas não possam utilizar os proxies.

Um outro problema dos proxies tradicionais, é que eles só podem ser utilizados para acessos de dentro para fora (não se pode solicitar para que clientes externos repassem suas solicitações para o seu proxy para que este repasse para seu servidor interno).

A figura abaixo ilustra o funcionamento básico de um proxy tradicional:

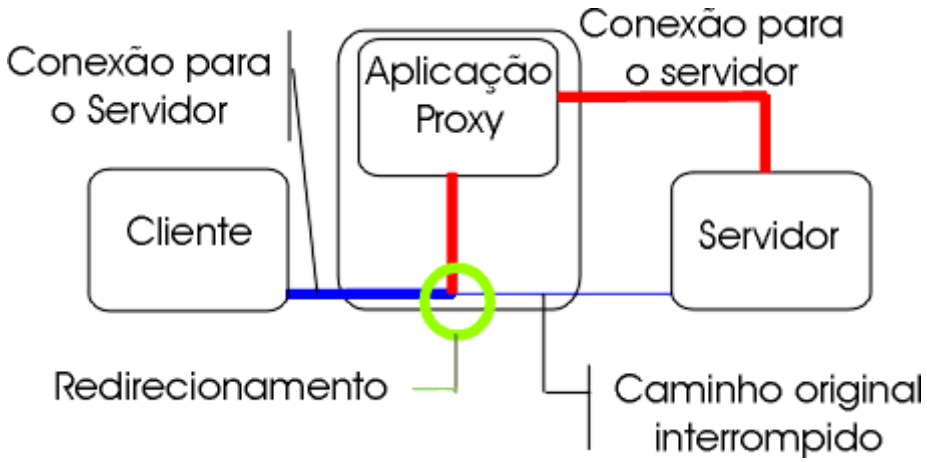


Proxies transparentes

O Firewall Aker introduz um novo conceito de firewall com a utilização de proxies transparentes. Estes proxies transparentes são capazes de serem utilizados sem nenhuma alteração nas máquinas clientes e nas máquinas servidoras, simplesmente porque nenhuma delas sabe de sua existência.

Seu funcionamento é igualmente simples: todas as vezes que o firewall decide que uma determinada conexão deve ser tratada por um proxy transparente, esta conexão é desviada para o proxy em questão. Ao receber a conexão, o proxy abre uma nova conexão para o servidor remoto e repassa as requisições do cliente para este servidor.

A grande vantagem desta forma de trabalho, é que se torna possível oferecer uma segurança adicional para certos serviços sem perda da flexibilidade e sem a necessidade de alteração de nenhuma máquina cliente ou servidora. Além disso, é possível se utilizar proxies transparentes em requisições de dentro para fora e de fora para dentro, indiferentemente.

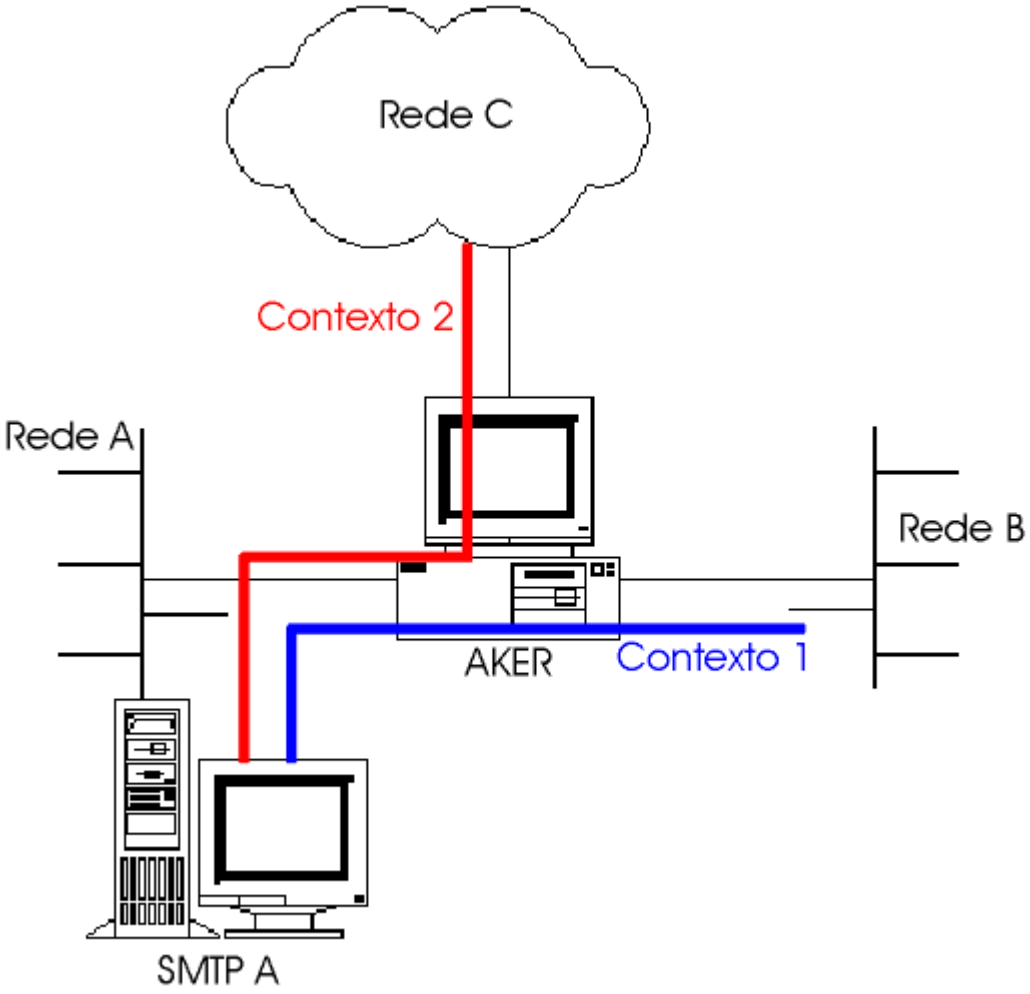


Proxies transparentes e contextos

O Firewall Aker introduz uma novidade com relação aos proxies transparentes: os contextos. Para entendê-los, vamos inicialmente analisar uma topologia de rede onde sua existência é necessária.

Suponha que exista um Firewall Aker conectado a três redes distintas, chamadas de redes ***A***, ***B*** e ***C,*** e que as redes *A* e *B* sejam redes de dois departamentos de uma mesma

empresa e a rede *C* a Internet. Suponha ainda que na rede *A* exista um servidor SMTP que seja utilizado também pela rede *B* para enviar e receber correio eletrônico. Isto está ilustrado no desenho abaixo:



Suponha agora que se deseje configurar o firewall para desviar todas as conexões SMTP para o proxy SMTP, de modo a assegurar uma maior proteção e um maior controle sobre este tráfego.

É importante que exista um meio de se tratar diferentemente as conexões para *A* com origem em *B* e *C*: a rede *B* utilizará o servidor SMTP de *A* como relay ao enviar seus e-mails, entretanto este mesmo comportamento não deve ser permitido a partir da rede *C*. Pode-se também querer limitar o tamanho máximo das mensagens originadas na rede *C*, para evitar ataques de negação de serviço baseados em falta de espaço em disco, sem ao mesmo tempo querer limitar também o tamanho das mensagens originadas na rede *B*.

Para possibilitar este tratamento diferenciado, foi criado o conceito de *contextos*. Contextos nada mais são que configurações diferenciadas para os proxies transparentes de modo a possibilitar comportamentos diferentes para conexões distintas.

No exemplo acima, poderia-se criar dois contextos: um para ser usado em conexões de *B* para *A* e outro de *C* para *A*.

Os proxies do Firewall Aker

O Firewall Aker implementa proxies transparentes para os serviços FTP, Telnet, SMTP, POP3, HTTP e RPC e proxies não transparentes para os serviços acessados através de um browser WWW (FTP, Gopher, HTTP e HTTPS) e para clientes que suportem o protocolo SOCKS. Para se utilizar os proxies não transparentes, é necessário um cliente que possa ser configurado para tal. Dentre os clientes que suportam este tipo de configuração, pode-se citar o Netscape Navigator(Tm) e o Internet Explorer(Tm).

Os proxies transparentes podem ser utilizados tanto para controlar acessos externos às redes internas quanto acessos de dentro para fora. Os proxies não transparentes somente podem ser usados de dentro para fora.

O Firewall Aker permite ainda implementar Proxies criados pelo usuário que são proxies criados por terceiros utilizando a API de desenvolvimento que a Aker Security Solutions provê. O objetivo é possibilitar que instituições que possuam protocolos específicos possam criar suporte no firewall para estes protocolos.

Os autenticadores do Firewall Aker

Os proxies SOCKS, Telnet e WWW do Firewall Aker suportam autenticação de usuários, isto é, podem ser configurados para só permitir que uma determinada sessão seja estabelecida caso o usuário se identifique para o firewall, através de um nome e uma senha, e este tenha permissão para iniciar a sessão desejada.

O grande problema que surge neste tipo de autenticação, é como o firewall irá validar os nomes e as senhas recebidas. Alguns produtos exigem que todos os usuários sejam cadastrados em uma base de dados do próprio firewall ou que sejam usuários válidos da máquina que o firewall estiver rodando. Ambos os métodos possuem o grande inconveniente de não aproveitar a base de usuários normalmente presente em uma rede local.

No Firewall Aker, optou-se por uma solução mais versátil e simples de ser implantada: ao invés de exigir um cadastramento de usuários no firewall, estes são validados nos próprios servidores da rede local, sejam estes Unix ou Windows NT.

Para que seja possível ao firewall saber em quais máquinas ele deve autenticar os usuários, e também para possibilitar uma comunicação segura com estas máquinas, foi criado o conceito de *autenticadores*. Autenticadores são máquinas Unix ou Windows NT, que rodam um pequeno programa chamado de *Agente de autenticação*. Este programa é distribuído como parte do Firewall Aker e tem como função básica servir de interface entre o firewall e a base de dados remota.

Para que o Firewall Aker utilize uma base de dados em um servidor remoto, deve-se efetuar os seguintes procedimentos:

1. Instalar e configurar o agente de autenticação na máquina onde reside a base de dados de usuários (este procedimento será descrito nos tópicos intitulados Instalando o agente de autenticação no Unix e Instalando o agente de autenticação no Windows NT).

2. Cadastrar uma entidade do tipo autenticador com o endereço da máquina onde o agente foi instalado e com a senha de acesso correta (para maiores informações de como cadastrar entidades, veja o capítulo intitulado Cadastrando Entidades).
3. Indicar para o firewall que ele deve utilizar o autenticador cadastrado no passo 2 para realizar a autenticação de usuários (este procedimento será descrito no capítulo intitulado Configurando parâmetros de autenticação).

O Firewall Aker 5.1 é incompatível com versões anteriores à 4.0 dos agentes de autenticação. Caso se tenha feito upgrade de uma versão anterior e se esteja utilizando autenticação, é necessário reinstalar os autenticadores.

É possível também se realizar autententicações através dos protocolos LDAP e RADIUS. Neste caso, não existe a necessidade de instalação dos autenticadores nas máquinas servidoras, bastando se criar os autenticadores dos tipos correspondentes e indicar ao firewall que eles devem ser utilizados, de acordo com os passos 2 e 3 listados acima.

18-2 Instalando o agente de autenticação em plataformas Unix

Para se instalar o agente de autenticação, é necessário montar o CD-ROM do Aker Security Suite na máquina que se deseja instalá-lo ou copiar o conteúdo do diretório de instalação do agente do CD-ROM para algum diretório temporário nesta máquina (é possível se realizar esta cópia via FTP ou NFS, caso não se possua um leitor de CD-ROM na máquina onde o agente será instalado).

Após se realizar a montagem do CD-ROM, ou a cópia dos arquivos para um diretório qualquer, deve-se executar o seguinte comando:

#*/diretorio_de_instalacao*/br/agente/*plataforma*/aginst

Onde *diretorio_de_instalacao* é o diretório onde se encontram os arquivos de instalação, *plataforma* é a plataforma desejada e *diretorio* o diretório de destino. Para se instalar, por exemplo, o agente para a plataforma FreeBSD e com o CD-ROM montado no diretório `/cdrom`, o comando a ser digitado seria:
#/cdrom/br/agente/freebsd/aginst

O símbolo # representa o prompt do shell quando executado como root, ele não deve ser digitado como parte do comando.

O programa de instalação copiará o executável do agente (*`fwagaut`*) para o diretório `/usr/local/bin` e copiará um modelo do arquivo de configuração (*`fwagaut.cfg`*) para o diretório `/etc/`. Após a instalação, é necessário se personalizar este arquivo, como descrito na próxima seção.

Caso se tenha respondido *"Sim"* quando o programa de instalação perguntou se o agente deveria ser iniciado automaticamente, uma chamada será criada em um arquivo de inicialização da máquina de modo a carregar automaticamente o agente. O nome deste arquivo de inicialização é dependente da versão de Unix utilizada.

A sintaxe do arquivo de configuração do agente de autenticação

Após se instalar o agente de autenticação, é necessário se criar um arquivo de configuração com o endereço dos firewalls que poderão utilizá-lo e a senha de acesso de cada um. Este arquivo é em formato texto e pode ser criado por qualquer editor.

O arquivo de configuração do agente de autenticação deve ter seus direitos configurados de forma que só o usuário root possa ler ou alterar seu conteúdo. Para fazer isso, pode-se usar o comando *chmod*, com a seguinte sintaxe: `#chmod 600 nome_do_arquivo`.

A sua sintaxe é a seguinte:

- Cada linha deve conter o endereço IP de um Firewall Aker que irá utilizar o agente, um ou mais espaços em branco ou caracteres *tab* e a senha de acesso que o firewall irá utilizar para a comunicação.
- Linhas começadas pelo caractere #, bem como linhas em branco, são ignoradas

Um exemplo de um possível arquivo de configuração é mostrado a seguir:

```
# Arquivo de configuracao do agente de autenticacao do Firewall Aker
5.1
#
# Sintaxe: Endereco IP do Firewall e senha de acesso (em cada linha)
#
# Obs: A senha nao pode conter espacos e deve ter ate 31 caracteres
#
# Linhas comecadas pelo caractere '#' sao consideradas comentarios
# Linhas em branco sao permitidas

10.0.0.1 teste_de_senha
10.2.2.2 123senha321
```

O local padrão para o arquivo de configuração do agente é **`/etc/fwagaut.cfg`**, entretanto é possível criá-lo com qualquer outro nome ou em outro diretório, desde que se informe isso ao agente no momento de sua execução. Isto será mostrado no tópico abaixo.

Sintaxe de execução do agente de autenticação

O agente de autenticação para Unix, possui a seguinte sintaxe de execução:

```
fwagaut [-?] [-c NOME_ARQUIVO] [-s <0-7>] [-q]
Onde:
      -? Mostra esta mensagem retorna ao prompt do shell
      -c Especifica o nome de um arquivo de configuracao alternativo
      -s Especifica a fila do syslog para onde devem ser enviadas as
         mensagens do autenticador. 0 = local0, 1 = local1, ...
      -r  Aceita validacao do usuario root
      -e  Aceita usuarios com senhas em branco
      -q  Nao mostra mensagem na hora da entrada
```

Suponha que o agente esteja localizado no diretório `/usr/local/bin` e que se tenha criado o arquivo de configuração com o nome `/usr/local/etc/fwagaut.cfg`. Neste caso, para executar o agente, a linha de comando seria:

```
/usr/local/bin/fwagaut -c /usr/local/etc/fwagaut.cfg
```

Caso se deseje executar o agente com o arquivo de configuração no local padrão, não é necessário a utilização da opção **`-c`**, bastando simplemente executá-lo com o comando:

```
/usr/local/bin/fwagaut
```

O agente de autenticação deve ser executado pelo o usuário root

Quando se fizer alguma alteração no arquivo de configuração, é necessário informar isso ao agente, se ele estiver rodando. Para tal, deve-se executar o seguinte comando:

```
#kill -1 pid
```

Onde *pid* é o número do processo do agente de autenticação. Para se obter este número, pode-se executar o comando **`#ps -ax | grep fwagaut`**, em máquinas baseadas em Unix BSD, ou **`#ps -ef | grep fwagaut`**, em máquinas baseadas em Unix System V.

O agente de autenticação escuta requisições na porta 1021/TCP. Não pode existir nenhuma outra aplicação utilizando esta porta enquanto o agente estiver ativo.

18-3 Instalando o agente de autenticação em Windows NT/2000

A instalação do agente de autenticação para NT é bastante simples. Para instalá-lo, é necessário colocar o CD-ROM do Firewall Aker 5.1 na máquina destino ou copiar o conteúdo do diretório de instalação do agente do CD-ROM para algum diretório temporário nesta máquina.

A seguir, deve-se clicar no menu *Iniciar*, selecionar a opção *Executar* e digitar o seguinte comando no campo *Abrir*: **`D:\br\agente\NT\setup`** (caso a unidade de CD-ROM seja diferente de **D**, substituir a letra D, pela letra equivalente).

O programa inicialmente mostrará uma janela pedindo uma confirmação para prosseguir com a instalação. Deve-se responder **Sim** para continuar com a instalação. A seguir será mostrada uma janela com a licença e por fim a janela onde se pode especificar o diretório de instalação. Essa janela possui o formato mostrado abaixo:

Instalação - Agente de Autenticação Aker
Selecione a unidade de disco e o diretório para a instalação do programa.
Diretório - C:\Arquivos de programas\Aker\FWNTAA
Procurar
Espaço necessário - 4 M
A unidade C: possui 1788 Mbytes disponíveis
Sair da Instalação
<< Último
Copiar Arquivos >>

Após se selecionar o diretório de instalação, deve-se pressionar o botão **Copiar arquivos**, que realizará toda a instalação do agente. Esta instalação consiste na criação de um diretório chamado de **fwntaa**, dentro do diretório **Arquivos de Programas**, com os arquivos do agente, a criação de um grupo chamado de *Firewall Aker* com as opções de configuração e remoção do agente e a criação de um serviço chamado de **Agente de autenticação do Firewall Aker**. Este serviço é um serviço normal do Windows NT e pode ser interrompido ou iniciado através do *Painel de Controle*, no ícone *serviços*.

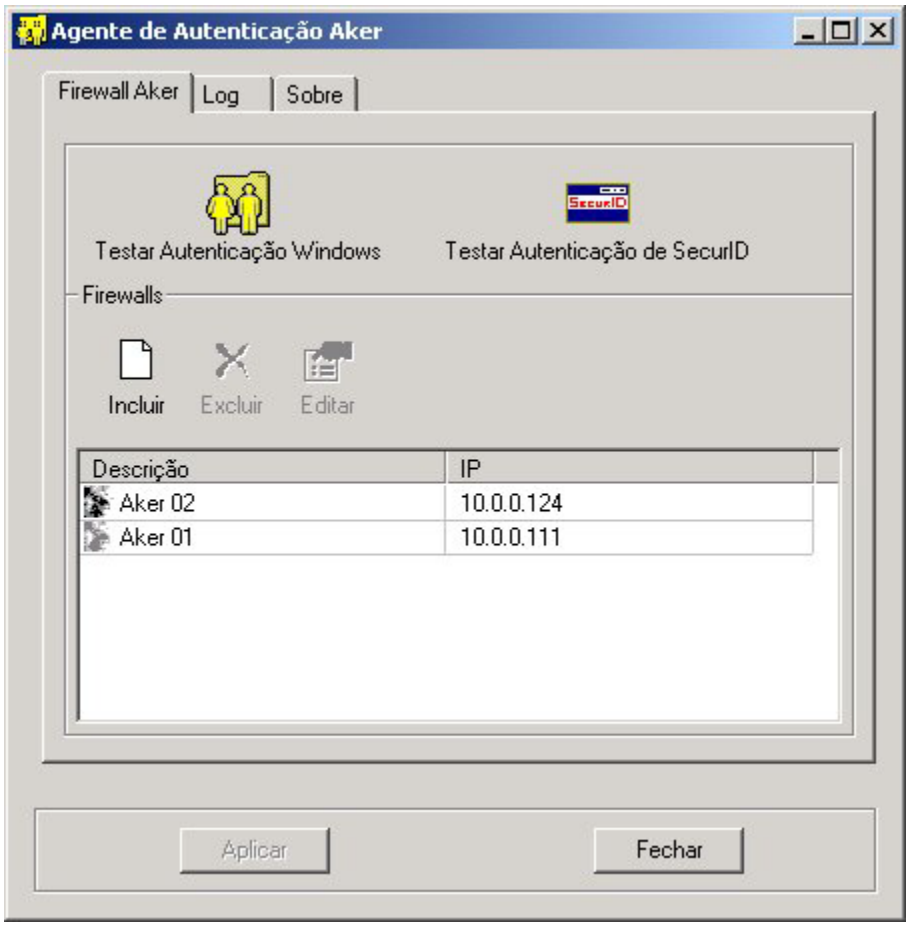
O agente de autenticação escuta requisições nas portas 1016/TCP e 1021/TCP. Não pode existir nenhuma outra aplicação utilizando estas portas enquanto o agente estiver ativo.

Configuração do agente de autenticação para NT

Após realizada a instalação do agente, é necessário se proceder com a sua configuração. Esta configuração permite se fazer o cadastramento de todos os firewalls que irão utilizá-lo, bem como a definição de que mensagens serão produzidas pelo agente, durante seu funcionamento. Ao contrário do agente de autenticação para Unix, esta configuração é feita através de um programa separado.

Para se ter acesso ao programa de configuração, deve-se clicar no menu *Iniciar*, selecionar o grupo *Firewall Aker* e dentro deste grupo a opção *Configurar agente de autenticação*. Ao ser feito isso, será mostrada a janela de configuração do agente, que consiste de três pastas:

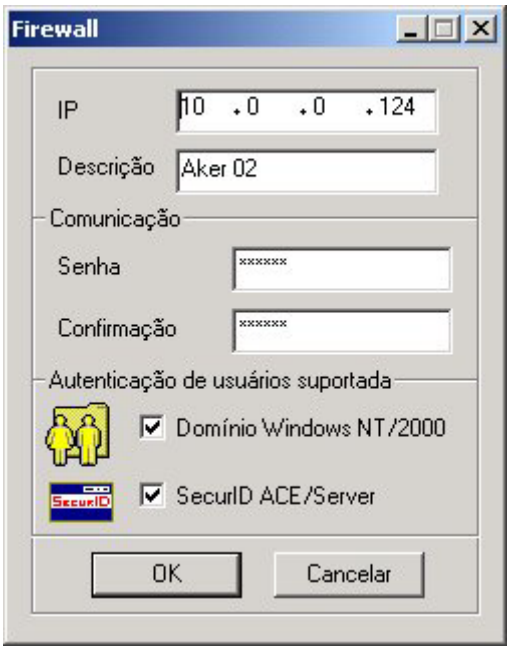
- **Pasta de configuração dos firewalls**



Esta pasta consiste em todas as opções de configuração do agente. Na parte superior existem dois botões que permitem testar a autenticação de um determinado usuário, a fim de verificar se o agente está funcionando corretamente. Na parte inferior da pasta existe uma lista com os firewalls autorizados a se conectarem ao agente de autenticação.

Para se incluir um novo firewall na lista, basta se clicar no botão **Incluir**, localizado na barra de ferramentas. Para se remover ou editar um firewall, basta se selecionar o firewall a ser removido ou editado e clicar na opção correspondente da barra de ferramentas.

No caso das opções *Incluir* ou *Editar* será mostrada seguinte janela:



IP: É o endereço IP do firewall que se conectará ao agente

Descrição: É um campo livre, utilizado apenas para fins de documentação

Senha: É a senha utilizada para gerar as chaves de autenticação e criptografia usadas na comunicação com o firewall. Esta senha deve ser igual à configurada na entidade do firewall. Para maiores informações, veja o capítulo intitulado Cadastrando Entidades.

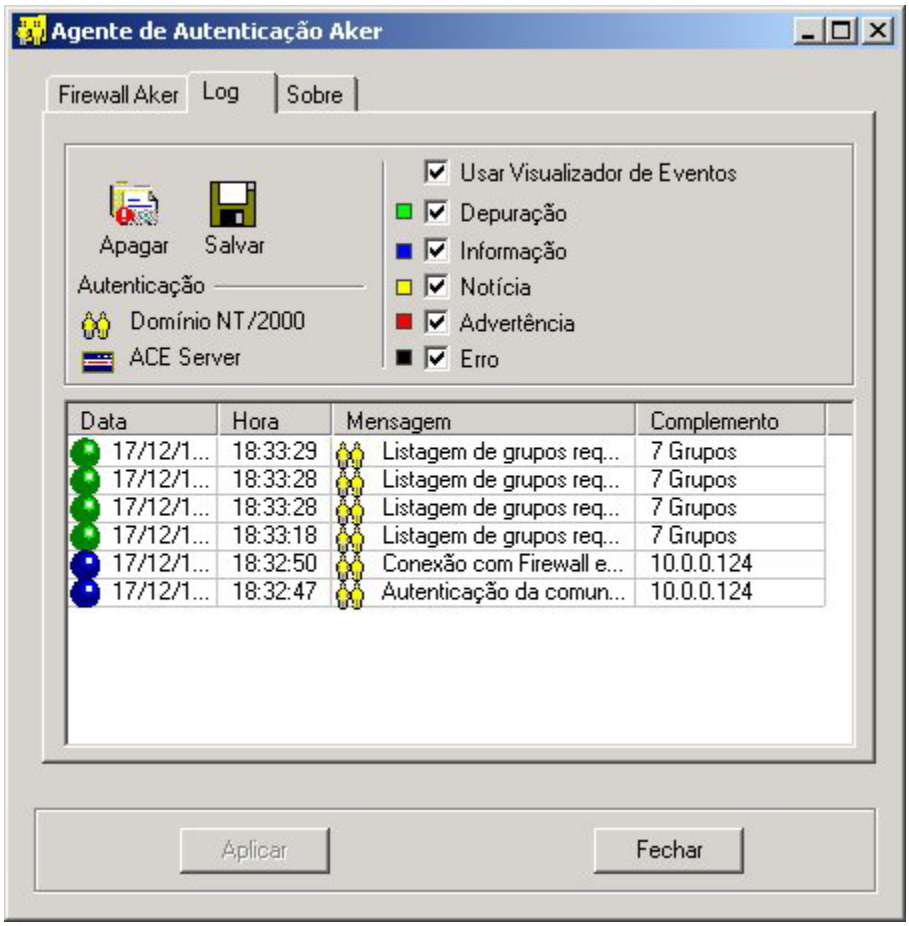
Confirmação: Este campo é utilizado apenas para se verificar se a senha foi digitada corretamente. Deve-se digitá-la exatamente como no campo *Senha*.

Autenticação de usuários suportada: Esse campo indica quais formas de autenticação de usuários serão permitidas. Ela consiste de duas opções que podem ser selecionadas independentemente:

Domínio Windows NT/2000: Se essa opção estiver marcada, o agente realizará autenticação de usuários utilizando a base de usuários do Windows NT/2000.

SecurID ACE/Server: Se essa opção estiver marcada, o agente realizará autenticação de usuários consultando o servidor SecurID.

- **Pasta de log**



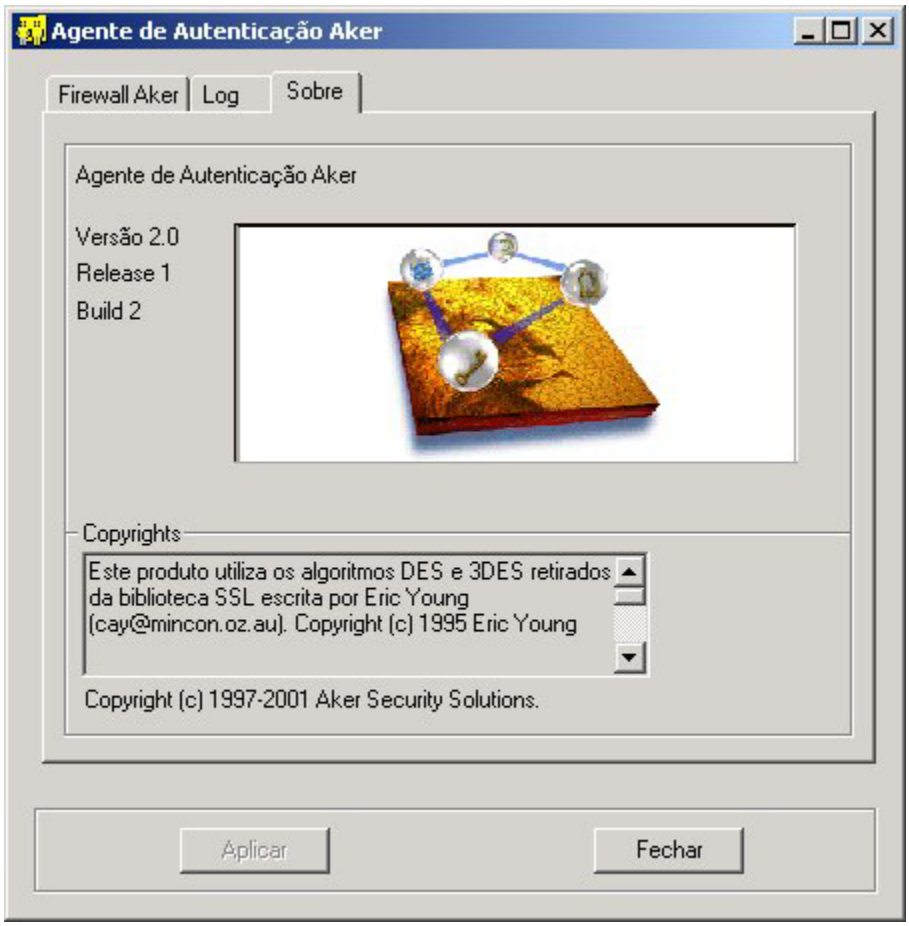
Esta pasta é muito útil para se acompanhar o funcionamento do agente de autenticação. Ela consiste de uma lista com diversas mensagens ordenadas pela hora. Ao lado de cada mensagem existe um ícone colorido, simbolizando sua prioridade. As cores tem o seguinte significado:

Verde	Depuração
Azul	Informação
Amarelo	Notícia
Vermelho	Advertência
Preto	Erro

Caso não se deseje que uma determinada prioridade de mensagens seja gerada, basta desmarcar a opção a sua esquerda.

A opção **Usar visualizador de eventos**, se estiver marcada, faz com que as mensagens sejam enviadas para o visualizador de eventos do Windows.

- **Pasta de sobre**



Esta é uma pasta meramente informativa e serve para que se obtenha algumas informações do cliente. Dentre as informações úteis se encontram sua versão e release.

Remoção do agente de autenticação para NT

Para facilitar a remoção do agente de autenticação para NT, existe um utilitário que a realiza automaticamente. Para iniciá-lo, deve-se clicar no menu *Iniciar*, selecionar o grupo *Firewall Aker* e dentro deste grupo a opção *Remover agente de autenticação*. Ao ser feito isso, será mostrada uma janela de confirmação.

Caso se deseje desinstalar o agente, deve-se clicar no botão **Sim**, caso contrário, deve-se clicar no botão **Não**, que cancelará o processo de remoção.

19-0 Configurando parâmetros de autenticação

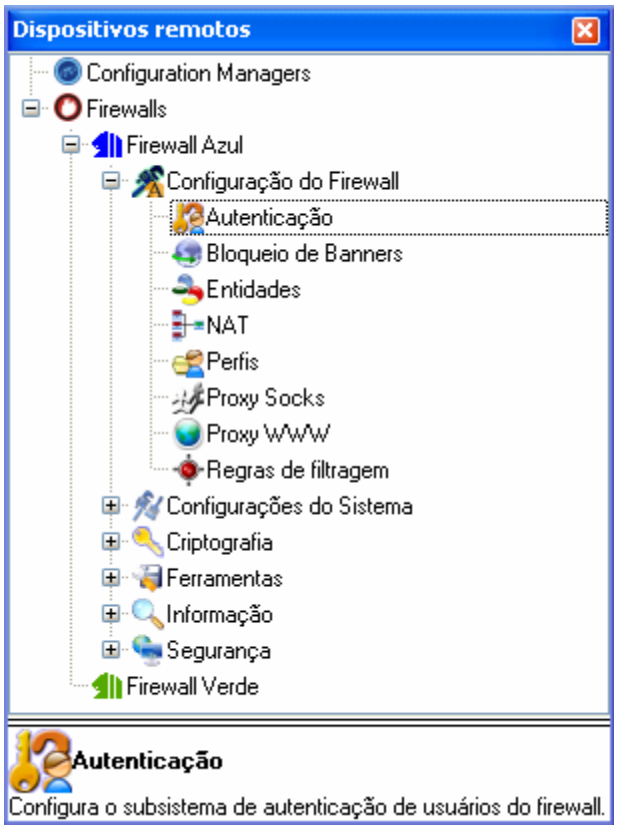
Neste capítulo serão mostrados quais são e como devem ser configurados os parâmetros de autenticação, essenciais para que seja possível a autenticação de usuários pelo firewall.

O que são os parâmetros de autenticação ?

Os parâmetros de autenticação servem para informar ao firewall que formas de autenticação são permitidas, quais autenticadores devem ser pesquisados na hora de autenticar um determinado usuário e em qual ordem. Além disso, eles controlam a forma com que a pesquisa é feita, permitindo uma maior ou menor flexibilidade para as autenticações.

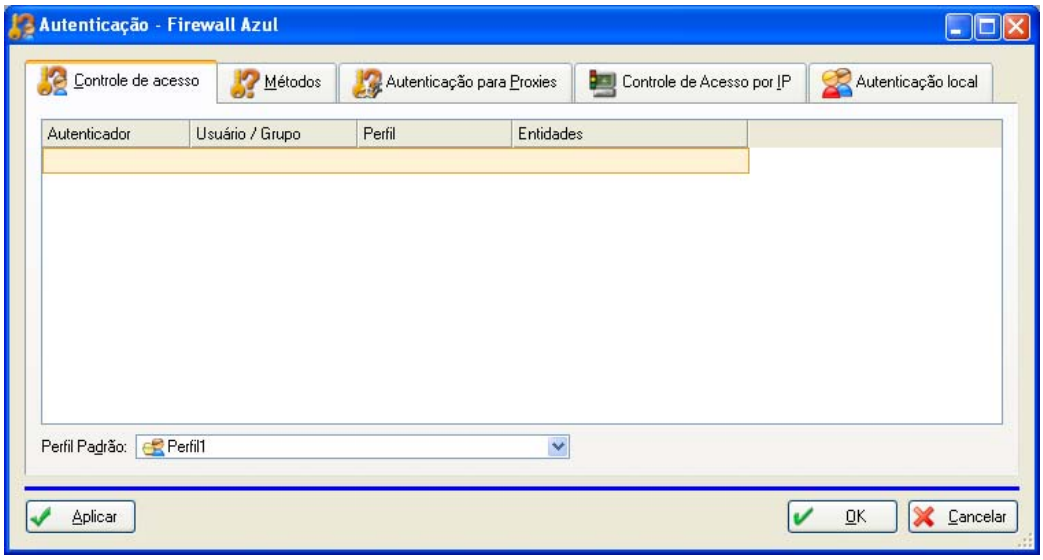
19-1 Utilizando a interface gráfica

Para ter acesso a janela de parâmetros de autenticação basta:



- Clicar no menu *Configuração do Firewall* da janela Firewalls
- Selecionar o item *Autenticação*

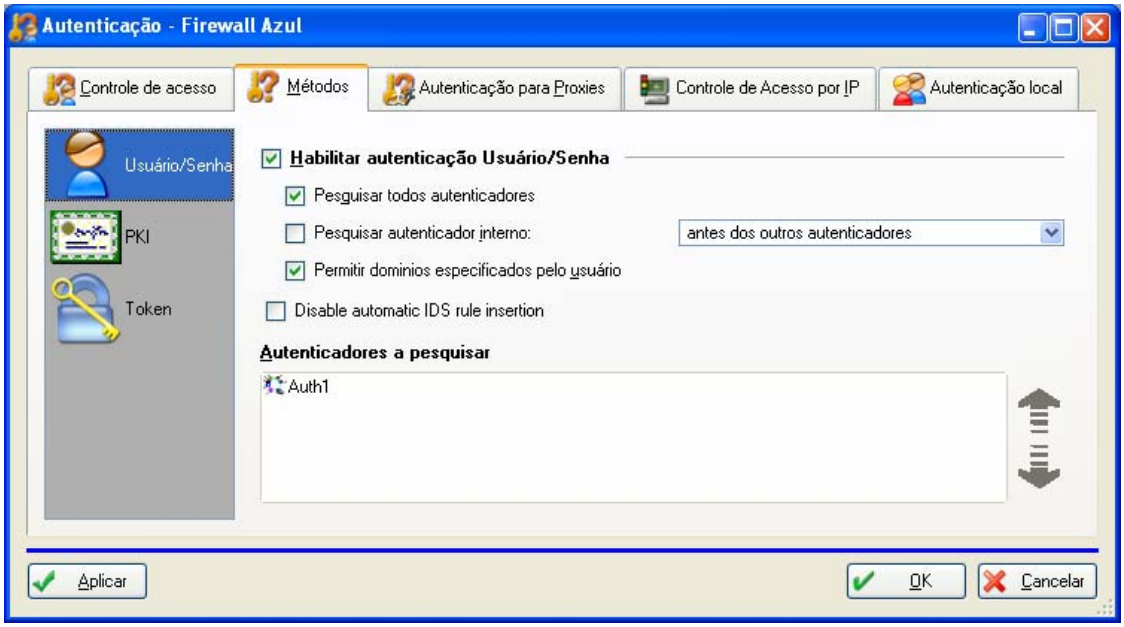
A aba de Controle de Acesso



Essa janela consiste de quatro partes distintas: a primeira aba corresponde ao **Controle de Acesso** onde os usuários e grupos de autenticadores são associados com perfis de acesso. A configuração desta aba será vista em detalhes em Perfis de Acesso de Usuários, na segunda aba escolhe-se os Métodos de autenticação onde se determina os parâmetros relativos à autenticação de usuários por meio de nomes/senhas e se configuram os parâmetros de autenticação por token (SecurID) e Autoridade Certificadora (PKI), a terceira aba configura-se a Autenticação para Proxies. Na quarta e última aba é configurado o Controle de Acesso por IP que também será visto com mais detalhes em Perfis de Acesso de Usuários.

- O botão **OK** fará com que a janela de configuração de parâmetros seja fechada e as alterações efetuadas aplicadas.
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta
- O botão **Cancelar** fará com que a janela seja fechada porém as alterações efetuadas não sejam aplicadas.

Aba Métodos



Habilita autenticação usuário/senha: Essa opção indica se o firewall aceitará ou não autenticação de usuários por meio de nomes/senhas. Caso ela esteja ativa, deve-se configurar os demais parâmetros relativos a esse tipo de autenticação:

Pesquisa em todos os autenticadores: Este parâmetro indica se o firewall deve tentar validar um usuário nos próximos autenticadores da lista no caso de um autenticador retornar uma mensagem de senha inválida.

Se esta opção estiver marcada, o firewall percorre todos os autenticadores da lista, um a um, até receber uma resposta de autenticação correta ou até a lista terminar. Caso ela não esteja marcada, a pesquisa será encerrada no primeiro autenticador que retornar uma mensagem de autenticação correta ou de senha inválida.

Esta opção só é usada para respostas de senha inválida. Caso um autenticador retorne uma resposta indicando que o usuário a ser validado não está cadastrado na base de dados de sua máquina, o firewall continuará a pesquisa no próximo autenticador da lista, independentemente do valor desta opção.

Pesquisa no autenticador local: Estê parâmetro indica se a base de usuários locais do firewall - definida na pasta Autenticação Local - deve ser consultada para validar a senha dos usuários. Se sim, também se deve escolher no combo box ao lado se essa base deve ser consultada antes ou depois dos demais autenticadores.

Usuário pode especificar domínio: Este parâmetro indica se o usuário na hora de se autenticar pode informar ao firewall em qual autenticador ele deseja ser validado.

Se esta opção estiver marcada, o usuário pode acrescentar juntamente ao seu nome, um sufixo formado pelo símbolo / e um nome de autenticador, fazendo com que a requisição de autenticação seja enviada diretamente para o autenticador informado. Caso ela não esteja marcada, a autenticação será feita na ordem dos autenticadores configurada pelo administrador.

O uso desta opção não obriga que o usuário informe o nome do autenticador, apenas permite que ele o faça, se desejar. Caso o usuário não informe, a autenticação seguirá na ordem normal.

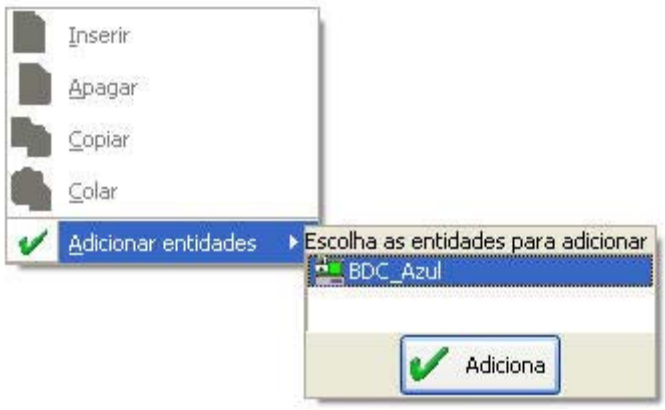
Para ilustrar a especificação de domínio, pode-se tomar como base um sistema no qual existam dois autenticadores configurados, chamados de *Unix* e *Windows_NT*. Neste sistema, se um usuário chamado *administrador* desejar se autenticar na máquina *Windows_NT*, então ele deverá entrar com o seguinte texto, quando lhe for solicitado seu login ou username: *administrador/Windows_NT*. Caso ele não informe o sufixo, o firewall tentará autenticá-lo inicialmente pela máquina *Unix* e caso não exista nenhum usuário cadastrado com este nome ou a opção *Pesquisa em todos os autenticadores* estiver marcada, ele então tentará autenticar pela máquina *Windows_NT*.

O nome do autenticador informado pelo usuário deve estar obrigatoriamente na lista de autenticadores a serem pesquisados.

Autenticadores a pesquisar

Para se incluir um autenticador na lista de autenticadores a serem consultados, deve-se proceder da seguinte forma:

1. Clicar com o botão direito do mouse onde aparecerá um menu suspenso (figura abaixo) ou arrastando a entidade autenticador para o local indicado



2. Seleciona-se o a opção **Adicionar entidades** e o autenticador a ser incluído, na lista mostrada à direita.

Para se remover um autenticador da lista de pesquisa, deve-se proceder da seguinte forma:

1. Seleciona-se o autenticador a ser removido e aperta-se a tecla delete ou
2. Clica-se no botão direito do mouse e seleciona-se no menu suspenso o item Apagar

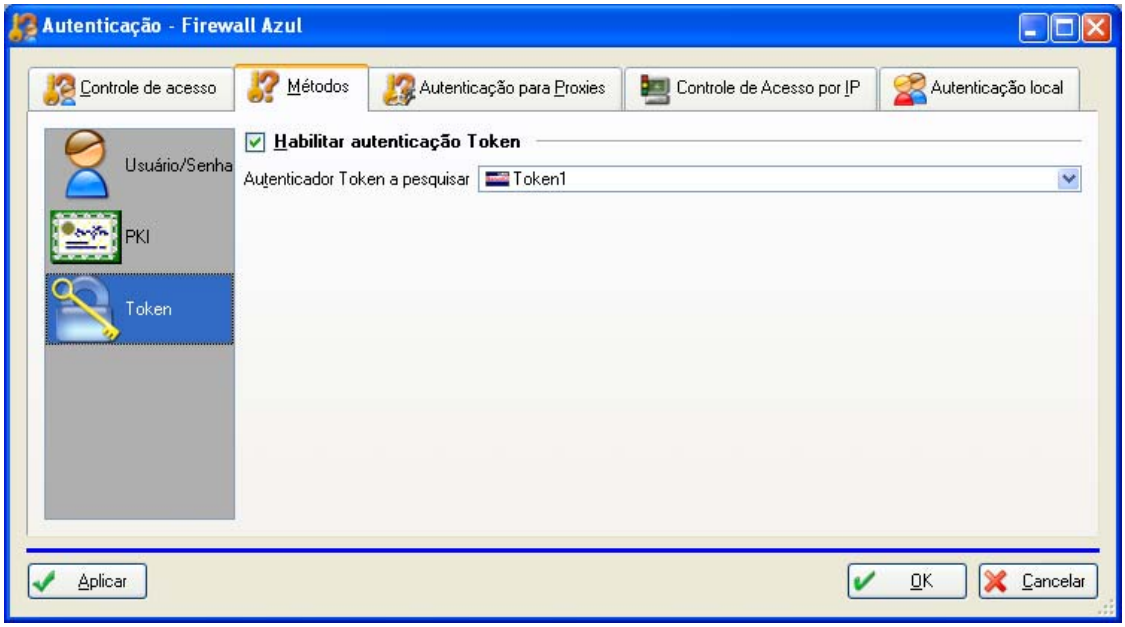
Para se mudar a ordem de pesquisa dos autenticadores, deve-se proceder da seguinte forma:

1. Seleciona-se o autenticador a ser mudado de posição na ordem de pesquisa.
2. Clica-se em um dos botões à direita da lista: o botão com o desenho da seta para cima fará com que o autenticador selecionado suba uma posição na lista. O botão com a seta para baixo fará com que ele seja movido uma posição para baixo na lista.

Dica: A adição ou remoção dos autenticadores pode ser feita diretamente com o mouse, bastando clicar e arrastar os mesmos para a janela correspondente, soltando em seguida.

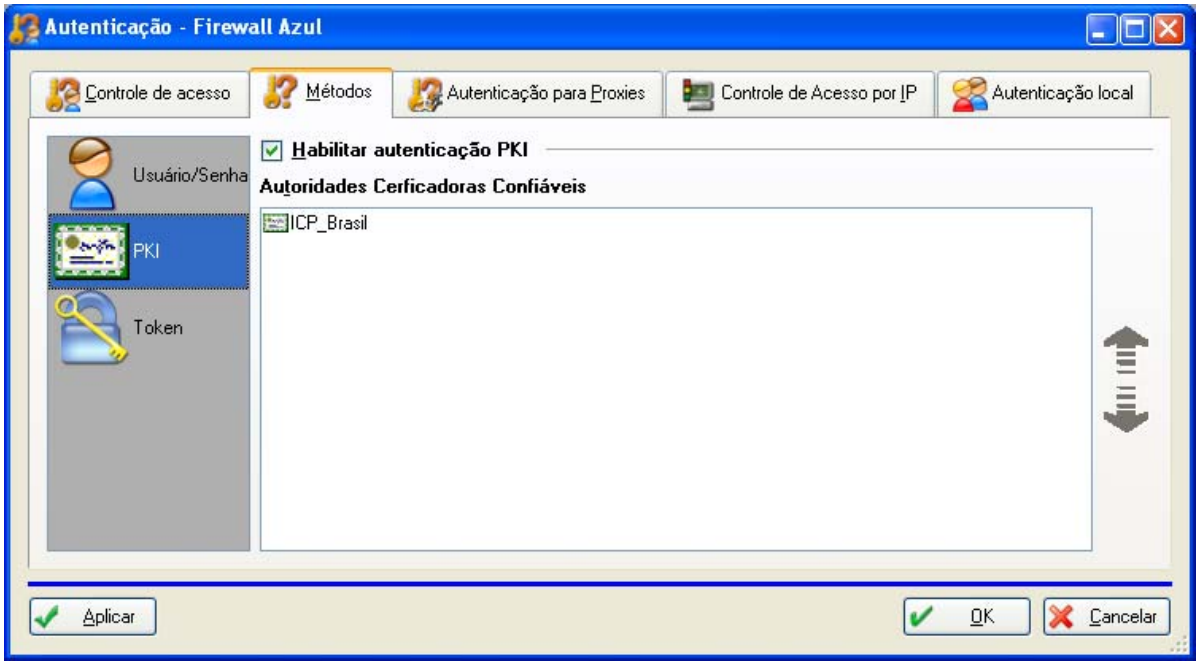
Os autenticadores serão pesquisados na ordem que se encontram na lista, de cima para baixo.

Habilita autenticação por token: Essa opção indica se o firewall aceitará ou não autenticação de usuários por meio de tokens. Caso ela esteja ativa, deve-se configurar o nome do autenticador token a ser consultado para validar os dados recebidos.



Autenticador token a pesquisar: Este campo indica o autenticador token para o qual os dados a serem validados serão repassados.

Habilita autenticação PKI: Essa opção indica se o firewall aceitará ou não autenticação de usuários por meio de smart cards. Caso ela esteja ativa, deve-se configurar as autoridades certificadoras nas quais o firewall confia.



Autoridades Certificadoras Confiáveis

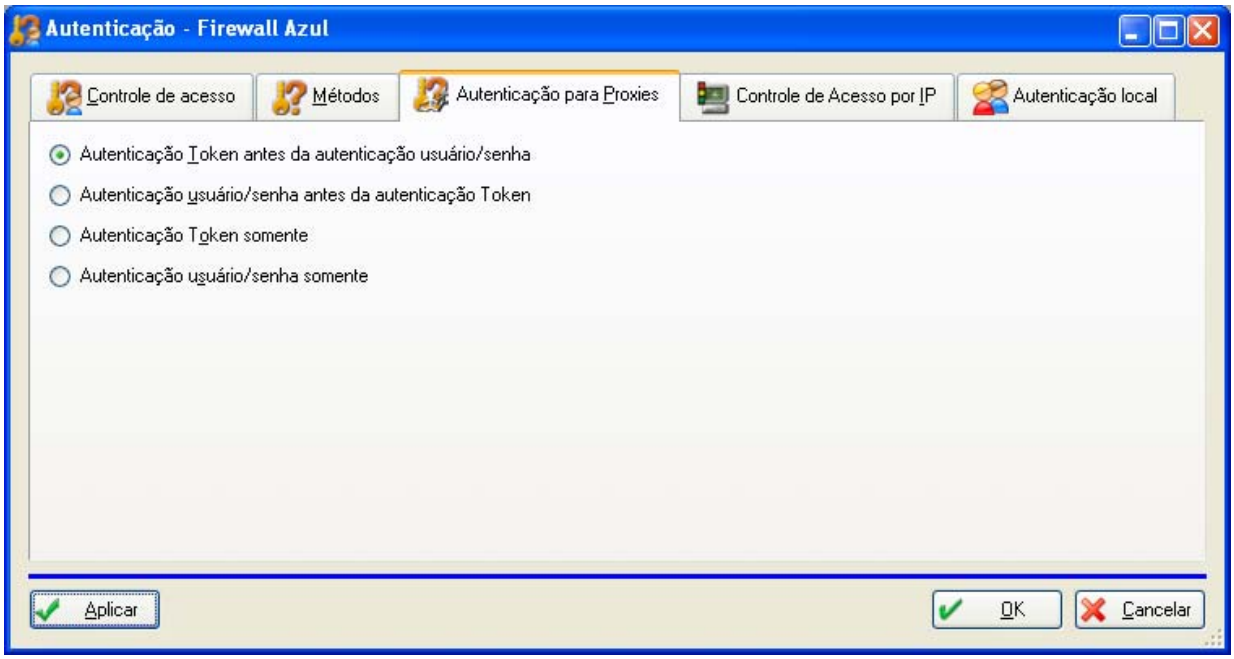
Para se incluir uma autoridade certificadora na lista de autoridades certificadoras confiáveis , deve-se proceder da seguinte forma:

1. Clica-se com o botão direito do mouse e escolhe-se a opção **Incluir Entidades**
2. Seleciona-se a autoridade a ser incluída
3. Clique em **Incluir**
4. Pode-se também clicar em uma autoridade certificadora e arrastá-la para posição desejada.

Para se remover uma autoridade certificadora da lista de autoridades confiáveis, deve-se proceder da seguinte forma:

1. Seleciona-se a autoridade a ser removida e aperta-se a tecla delete ou
2. Clica-se no botão direito do mouse sobre a entidade a ser removida e escolhe-se a opção **Apagar**

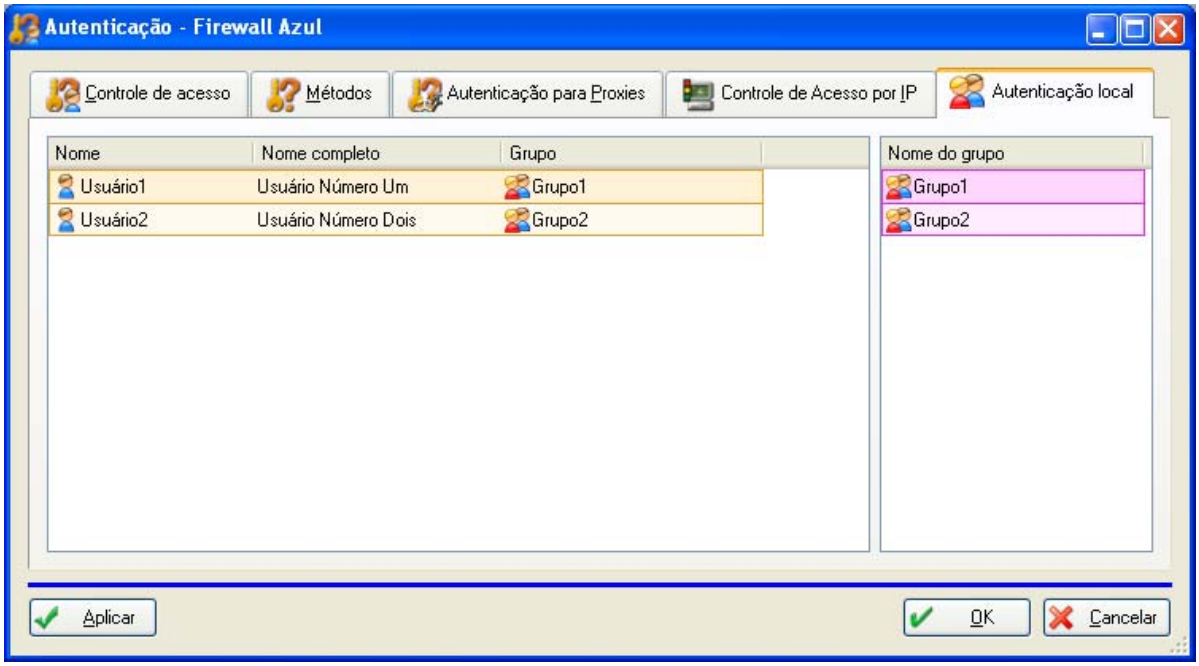
Autenticação para proxies



Estes parâmetros indicam que tipos de autenticação serão aceitas nos proxies e em que ordem serão validadas. Isso é importante pois quando um usuário é autenticando através de um browser, por exemplo, não é possível que ele especifique se está utilizando token ou usuário/senha. As opções possíveis da configuração são:

- Autenticador Token antes da autenticação usuário/senha
- Autenticação usuário/senha antes do autenticador token
- Somente autenticação por Token
- Somente autenticação usuário/senha

Autenticação Local

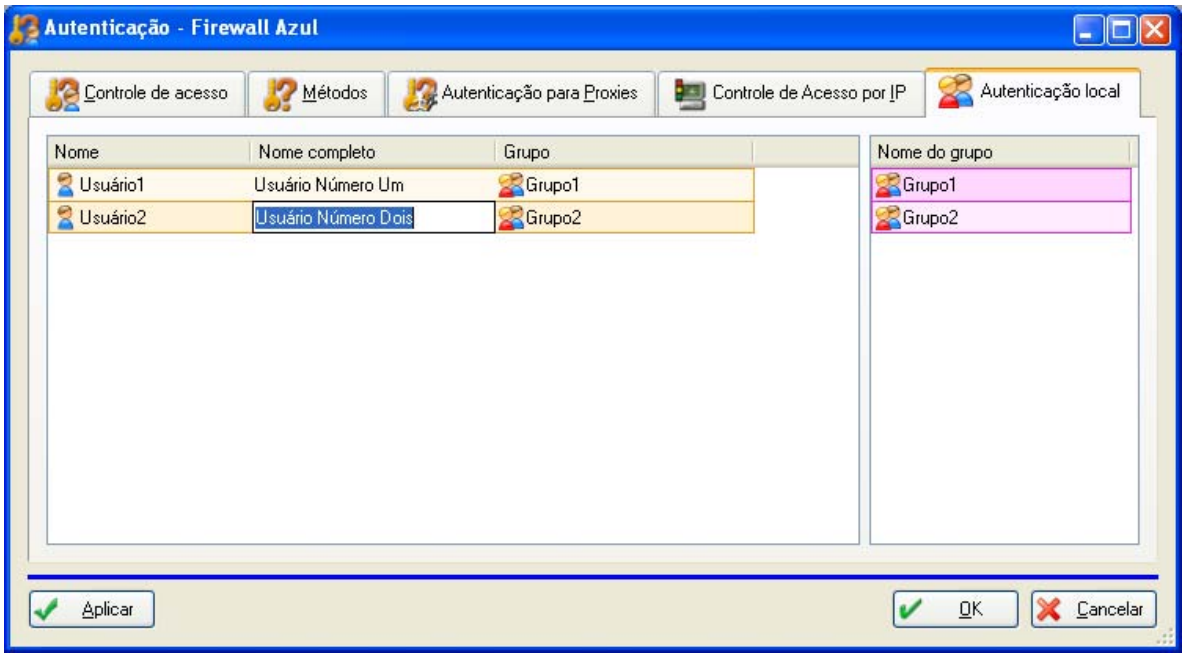


Nessa pasta, se pode cadastrar uma série de usuários e associar um grupo a cada um

deles. Se a opção de usar a base local de usuários estiver habilitada, então esses usuários também serão verificados como se estivessem em um autenticador remoto. Eles compõem o autenticador local.

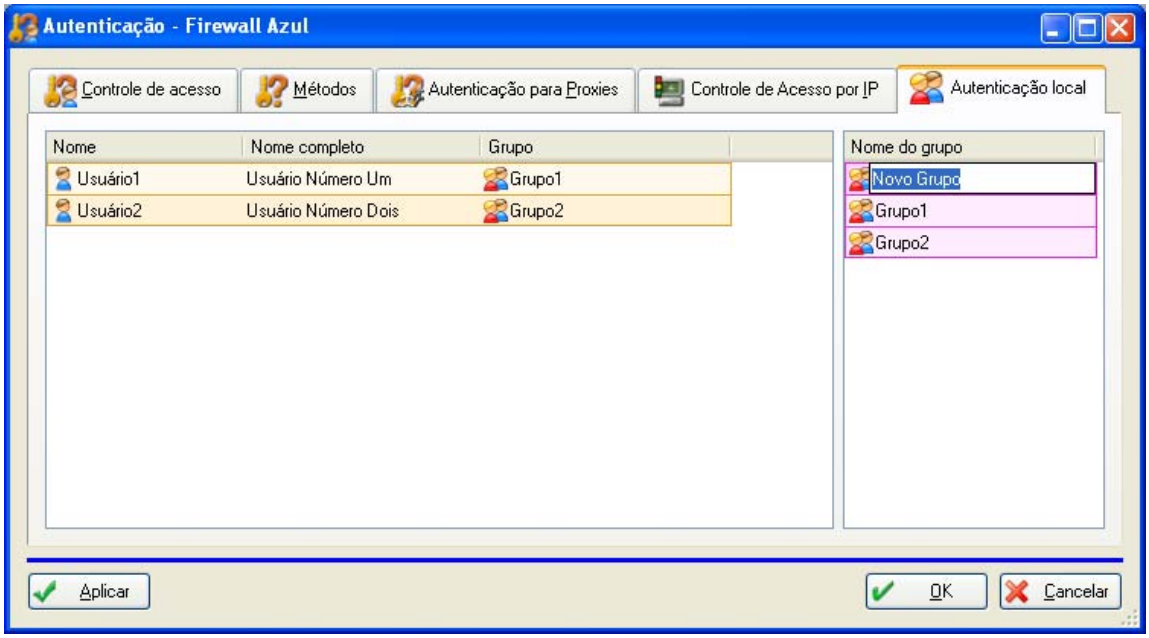
Para incluir um usuário, clique com o botão da direita e escolha inserir, ou então use o toolbar e clique no botão inserir: Você ainda pode usar o botão *insert* no seu teclado.

Para alterar o nome do usuário e seu nome completo, basta dar um duplo clique no campo correspondente:



Para alterar a senha ou o grupo a que está associado o usuário, use o menu de contexto sobre o ítem, clicando com o botão direito do mouse.

Para criar ou remover grupos, o procedimento é o mesmo, mas na lista lateral direita.



Grupos vazios não serão mantidos pelo firewall, apenas aqueles que contiverem ao menos um usuário.

19-2 Utilizando a interface texto

A interface texto permite configurar que tipo de autenticação será realizada e a ordem de pesquisa dos autenticadores.

Localização do programa: `/etc/firewall/fwauth`

Sintaxe:

```
Uso: fwauth [mostra | ajuda]
     fwauth [inclui | remove] [ca | token | autenticador] <entidade>
     fwauth [dominio | pesquisa_todos] [sim | nao]
```

```
     fwauth proxy [token | senha] [sim | nao]
     fwauth proxy primeiro [token | senha]
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
fwauth - Configura parametros autenticacao
Uso: fwauth [mostra | ajuda]
     fwauth [inclui | remove] [ca | token | autenticador] <entidade>
     fwauth [dominio | pesquisa_todos] [sim | nao]
     fwauth proxy [token | senha] [sim | nao]
     fwauth proxy primeiro [token | senha]

     mostra         = mostra a configuracao atual
     ajuda          = mostra esta mensagem
     inclui         = inclui entidade na lista de autenticadores
ativos
     remove         = remove entidade da lista de autenticadores
ativos
     dominio        = configura se o usuario pode ou nao especificar
dominio
     pesquisa_todos = configura se deve pesquisar em todos os
autenticadores
     proxy senha    = habilita autenticacao por proxies do tipo
usuario/senha
     proxy token    = habilita autenticacao por proxies do tipo Token
     proxy primeiro = configura qual o primeiro tipo de autenticacao a
ser usado
```

Exemplo 1: (mostrando os parâmetros de autenticação)

```
#fwauth mostra
AUTENTICACAO USUARIO/SENHA:
---------------------------
Pesquisa em todos autenticadores: sim
Usuario pode especificar dominio: nao
Autenticadores cadastrados:
aut_local

AUTENTICACAO PKI:
-----------------
Nao ha autenticadores cadastrados

AUTENTICACAO SECURY ID:
-----------------------
Nao ha autenticadores cadastrados
```

Exemplo 2: (incluindo um autenticador na lista de autenticadores ativos)

```
#fwauth inclui autenticador "agente 10.0.0.12"
Autenticador incluido
```

20-0 Perfis de Acesso de Usuários

Neste capítulo mostraremos para que servem e como configurar perfis de acesso no Firewall Aker

20-1 Planejando a instalação

O que são perfis de acesso ?

Firewalls tradicionais baseiam suas regras de proteção e controle de acesso a partir de máquinas, através de seus endereços IP. Enquanto que o Firewall Aker permite este tipo de controle, ele também permite que se defina controle de acesso por usuários. Desta forma, é possível que determinados usuários tenham seus privilégios e restrições garantidos, independentemente de qual máquina estejam utilizado em um determinado momento. Isso oferece o máximo em flexibilidade e segurança.

Para possibilitar este controle de acesso a nível de usuários, o Firewall Aker introduziu o conceito de perfis de acesso. Perfis de acesso representam os direitos a serem atribuídos a um determinado usuário no firewall. Estes direitos de acesso englobam todos os serviços suportados pelo firewall, o controle de páginas WWW e o controle de acesso através do proxy SOCKS. Desta forma, a partir de um único local, se consegue definir exatamente o que pode e não pode ser acessado.

Como funciona o controle com perfis de acesso ?

Para se utilizar os perfis de acesso, inicialmente cadastra-se os perfis desejados e posteriormente associa-se estes perfis com usuários e grupos de um ou mais autenticadores. A partir deste momento, todas as vezes que um usuário se logar no firewall com o Cliente de Autenticação Aker, Cliente de Criptografia Aker ou outro produto que ofereça funcionalidade equivalente, o firewall identificará o perfil de acesso correspondente a este usuário e configurará as permissões de acesso de acordo com este perfil. Tudo é feito de forma completamente transparente para o usuário final.

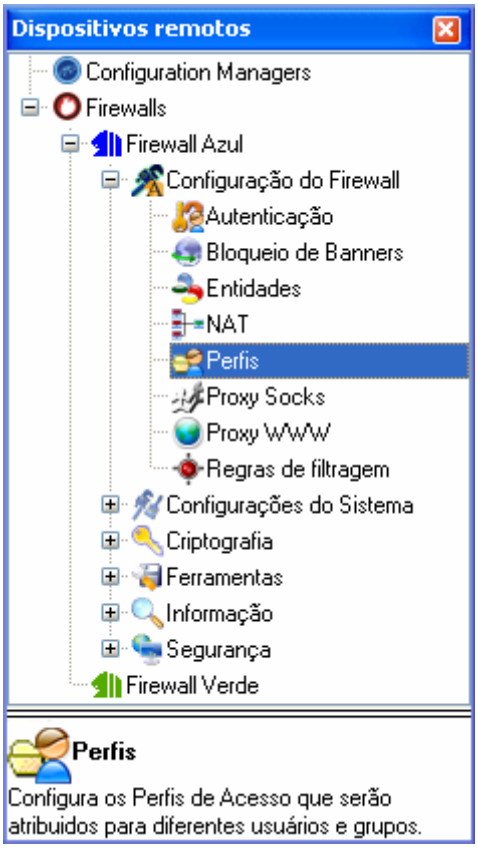
Para que seja possível o uso de perfis de acesso, é necessário que o Cliente de Autenticação ou o Cliente de Criptografia Aker estejam instalados em todas as máquinas clientes ou que se use a opção de autenticação por Java no proxy HTTP. Caso contrário, só será possível a utilização de controle de acesso a páginas WWW ou a serviços através do proxy SOCKS. A autenticação de usuários através dos proxies WWW (sem Java) e SOCKS é possível na medida em que eles solicitarão um nome de usuário e uma senha e pesquisarão o perfil correspondente quando não identificarem uma sessão ativa para uma determinada máquina.

20-2 Cadastrando perfis de acesso

Os perfis de acesso do Firewall Aker definem que páginas WWW podem ser visualizadas e que tipos de serviço podem ser acessados. Para cada página WWW ou

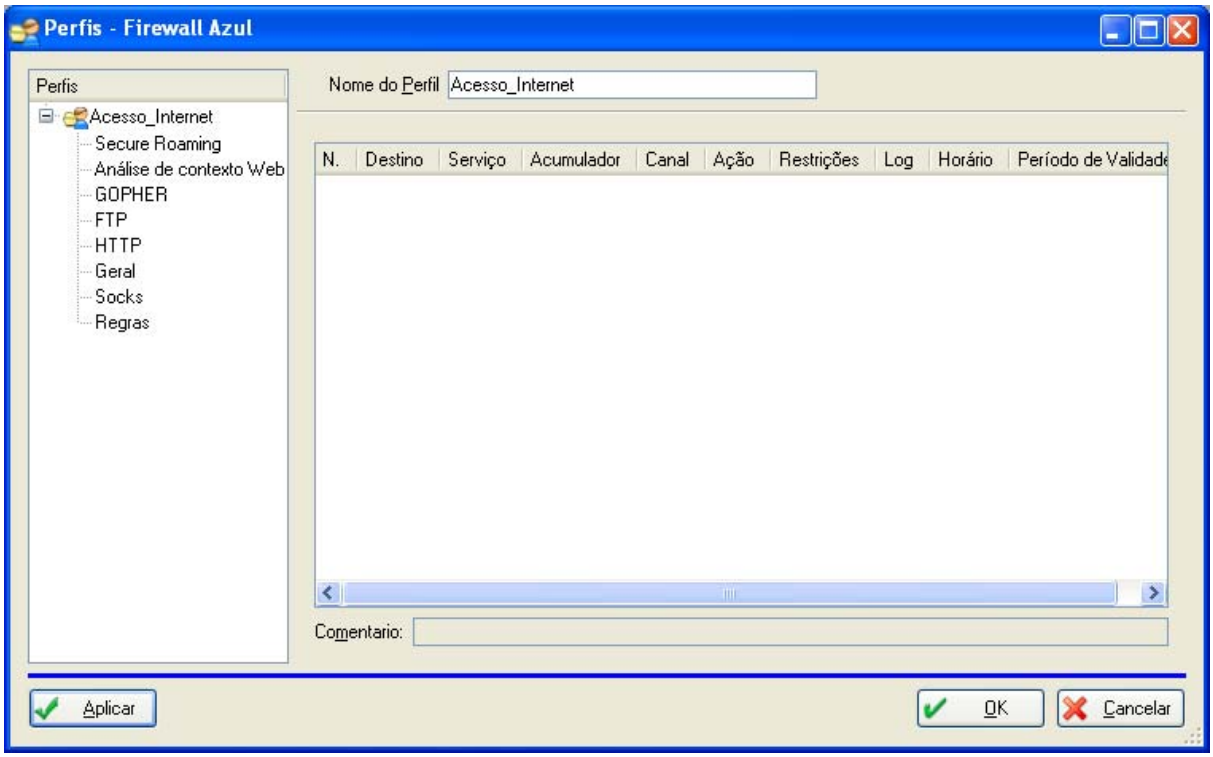
serviço, existe uma tabela de horários associada, através da qual é possível se definir os horários nos quais o serviço ou página pode ser acessado.

Para ter acesso à janela de perfis de acesso basta:



- Clicar no menu *Configuração do Firewall* da janela de administração do firewall
- Selecionar o item *Perfis*

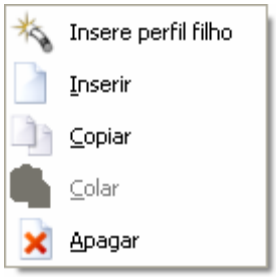
A janela de Perfis



A janela de perfis contém todos os perfis de acesso definidos no Firewall Aker. Ela consiste de uma lista onde cada perfil é mostrado em uma linha separada.

- O botão **OK** fará com que a janela de perfis seja fechada
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

Para se executar qualquer operação sobre um determinado perfil, basta clicar sobre ele e a seguir clicar na opção correspondente na barra de ferramentas. As seguintes opções estão disponíveis:



- **Incluir:** Esta opção permite se incluir um novo perfil na lista.
- **Excluir**: Esta opção remove da lista o perfil selecionado.
- **Copiar:** Esta opção copia o perfil selecionado para uma área temporária.
- **Colar:** Esta opção copia o perfil da área temporária para a lista.
- **Inserir perfil filho**: Esta opção inclui um novo perfil que é filho do perfil atual, i.e., estabelece uma hierarquia de perfis
- **Imprimir:** Gera relatório da lista de perfis em um documento html.

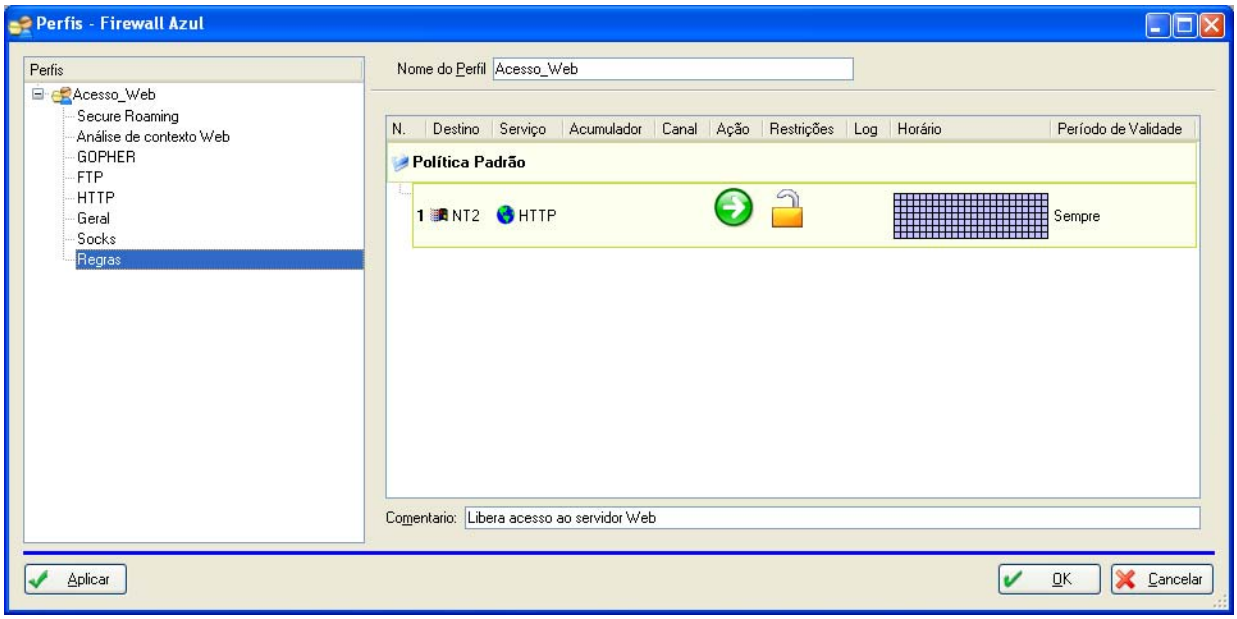
Para se excluir um perfil de acesso, ele não poderá estar associado a nenhum usuário (para maiores informações veja o tópico Associando Usuários com Perfis de Acesso)

O perfil filho, criado com a opção *Inserir perfil filho* herdará automaticamente as configurações do perfil pai.

Na parte superior de ambas as pastas, se encontra o campo **Nome**, que serve para se especificar o nome que identificará unicamente o perfil de acesso. Este nome será mostrado na lista de perfis e na janela de controle de acesso. Não podem existir dois perfis com o mesmo nome.

Cada perfil de acesso é composto de sete tópicos diferentes. Dependendo do tópico selecionado em um momento, a parte direita da janela mudará de modo a mostrar as diferentes opções. Os tópicos de configuração são:

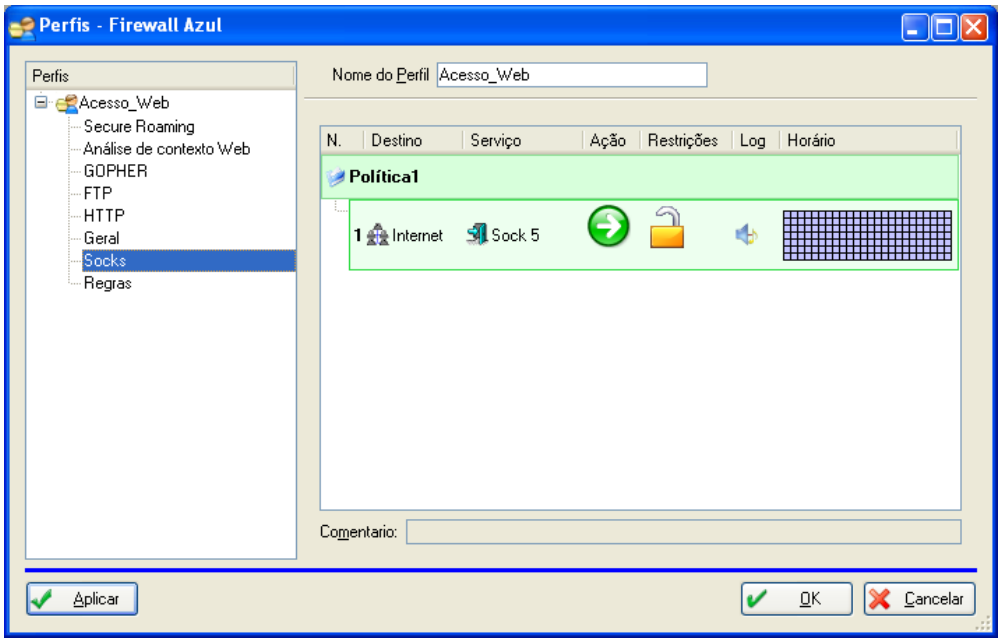
Regras



A pasta de regras permite que se especifique regras de filtragem para o perfil de acesso. Seu formato é exatamente igual à janela de regras de filtragem com a única excessão de que não se deve especificar entidades origem para a regra. Aqui também é possível trabalhar com Políticas de Regras de Filtragem. (para maiores informações, consulte o capítulo intitulado Filtro de Estados).

As regras de filtragem para os perfis de acesso consideram como origem a máquina na qual a sessão foi estabelecida. Devido a isso, é necessário apenas se especificar as entidades destino e serviços que podem ser acessados.

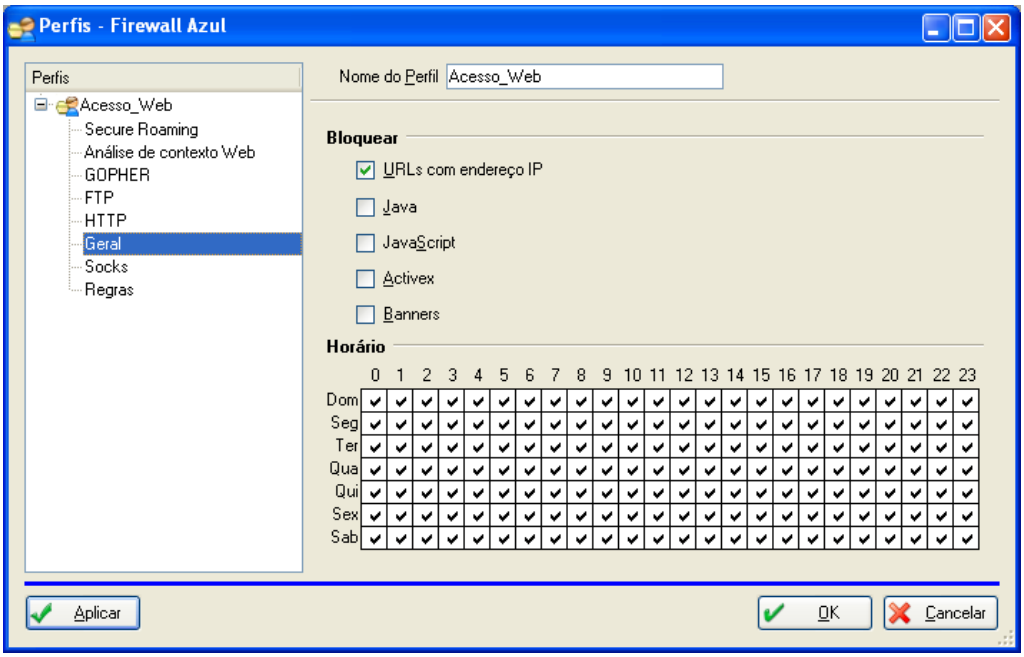
Regras SOCKS



A pasta de regras SOCKS permite que se especifique regras de filtragem para o acesso através do proxy SOCKS. Seu formato é exatamente igual à janela de regras de filtragem com a única exceção de que não se deve especificar entidades origem para a regra (para maiores informações, consulte o capítulo intitulado Filtro de Estados).

As regras de filtragem para o proxy SOCKS consideram como origem a máquina na qual a sessão foi estabelecida. Devido a isso, é necessário apenas se especificar as entidades destino e serviços que podem ser acessados.

Geral



As opções gerais de filtragem são definidas pelos seguintes campos:
Bloquear: Este campo define as opções de bloqueio em sites WWW. Sao elas:

- **URLs com endereço IP:** Se esta opção estiver marcada, não será permitido o acesso a URLs com endereços IP ao invés de nome (por exemplo, http://127.0.0.1/index.html), ou seja, somente será possível se acessar URLs por nomes.

Caso se tenha configurado o proxy WWW para fazer filtragem de URLs, deve-se configurar esta opção de modo ao usuário não poder acessar através de endereços IP, caso contrário, mesmo com o nome bloqueado, o usuário continuará podendo acessar a URL através de seu endereço IP. É possível se acrescentar endereços IP nas regras de filtragem WWW do perfil (caso se deseje realizar filtragem com esta opção ativa), entretanto, devido a estes sofrerem mudanças e ao fato de muitos servidores terem mais de um endereço IP, isto se torna extremamente difícil.

Por outro lado, muitos administradores percebem que sites mal configurados (especialmente os de webmail) utilizam redirecionamento para servidores pelo seu endereço IP, de forma que, com esta opção desmarcada, tais sites ficam inacessíveis.

- **Java, Javascript e Activex:** Estes campo permite se definir uma filtragem especial para páginas WWW, bloqueando, ou não, tecnologias consideradas perigosas ou incômodas para alguns ambientes. Ela possui quatro opções que podem ser selecionadas independentemente: **Javascript**, **Java** e **ActiveX**.

A filtragem de Javascript, Java e ActiveX é feita de forma com que a página filtrada seja visualizada como se o *browser* da máquina cliente não tivesse suporte para a(s) linguagem(ns) filtrada(s). Em alguns casos, isto pode fazer com que as páginas percam sua funcionalidade.

- **Banners:** Esta opção realiza o bloqueio de banners publicitários em páginas Web. Caso ela esteja marcada, o firewall substituirá os banners por espaços vazios na página, diminuindo o seu tempo de carga.

Uma vez configurado que se deve realizar o bloqueio, o mesmo será feito através de regras globais, iguais para todos os perfis. Para configurar estas regras de bloqueio de banners, basta:

- Clicar no menu *Configurações* da janela principal
- Selecionar o item *Bloqueio de banners*

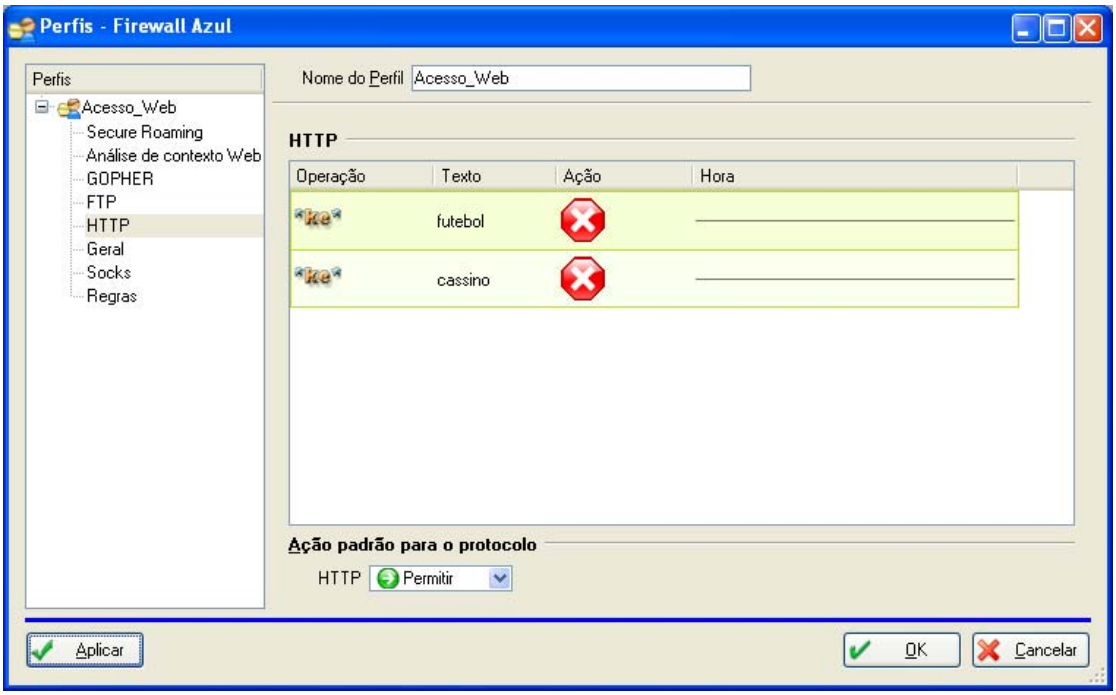
A janela abaixo irá ser mostrada:

Esta janela é formada por uma série de regras no formado de expressão regular. Caso uma URL se encaixe em qualquer regra, a mesma será considerada um banner e será bloqueada.

Horário padrão: Esta tabela define o horário padrão para as regras de filtragem WWW. Posteriormente, ao se incluir regras de filtragem WWW, existe a opção de se utilizar este horário padrão ou especificar um horário diferente.

As linhas representam os dias da semana e as colunas as horas. Caso se deseje que a regra seja aplicável em determinada hora então o quadrado deve ser preenchido, caso contrário o quadrado deve ser deixado em branco. Para facilitar sua configuração, pode-se clicar com o botão esquerdo do mouse sobre um quadrado e a seguir arrastá-lo, mantendo o botão pressionado. Isto faz com que o a tabela seja alterada na medida em que o mouse se move.

HTTP/FTP/GOPHER



A pasta de filtragem HTTP/FTP/GOPHER permite a definição de regras de filtragem de URLs para os protocolos HTTP/HTTPS, FTP e Gopher. Ela consiste de uma lista onde cada regra é mostrada em uma linha separada.

O protocolo HTTPS, para a URL inicial, é filtrado como se fosse o protocolo HTTP. Além disso, uma vez estabelecida a comunicação não é mais possível para o firewall filtrar qualquer parte de seu conteúdo, já que a criptografia é realizada diretamente entre o cliente e o servidor.

Na parte inferior da pasta existe um grupo que define a ação a ser executada caso o endereço que o cliente desejou acessar não se encaixe em nenhuma regra de filtragem. Este grupo é chamado de **Ação padrão para o protocolo** e consiste de três opções.

Permitir: Se esta opção for a selecionada, então o firewall aceitará as URLs que não se enquadrarem em nenhuma regra.

Bloquear: Se esta opção for a selecionada, então o firewall rejeitará as URLs que não se enquadrarem em nenhuma regra.

Categorizar: Se esta opção for a selecionada, então o firewall enviará as URLs que não se enquadrarem em nenhuma regra para serem analisadas pelo Analisador de URLs Aker.

Para se executar qualquer operação sobre uma determinada regra, basta clicar sobre ela e a seguir clicar na opção correspondente na barra de ferramentas. As seguintes opções estão disponíveis:

- **Inserir:** Esta opção permite se incluir uma nova regra na lista. Se alguma regra estiver selecionada, a nova será inserida na posição da regra selecionada. Caso contrário, a nova regra será incluída no final da lista.

- **Apagar:** Esta opção remove da lista a regra selecionada.
- **Copiar:** Esta opção copia a regra selecionada para uma área temporária.
- **Colar:** Esta opção copia a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.

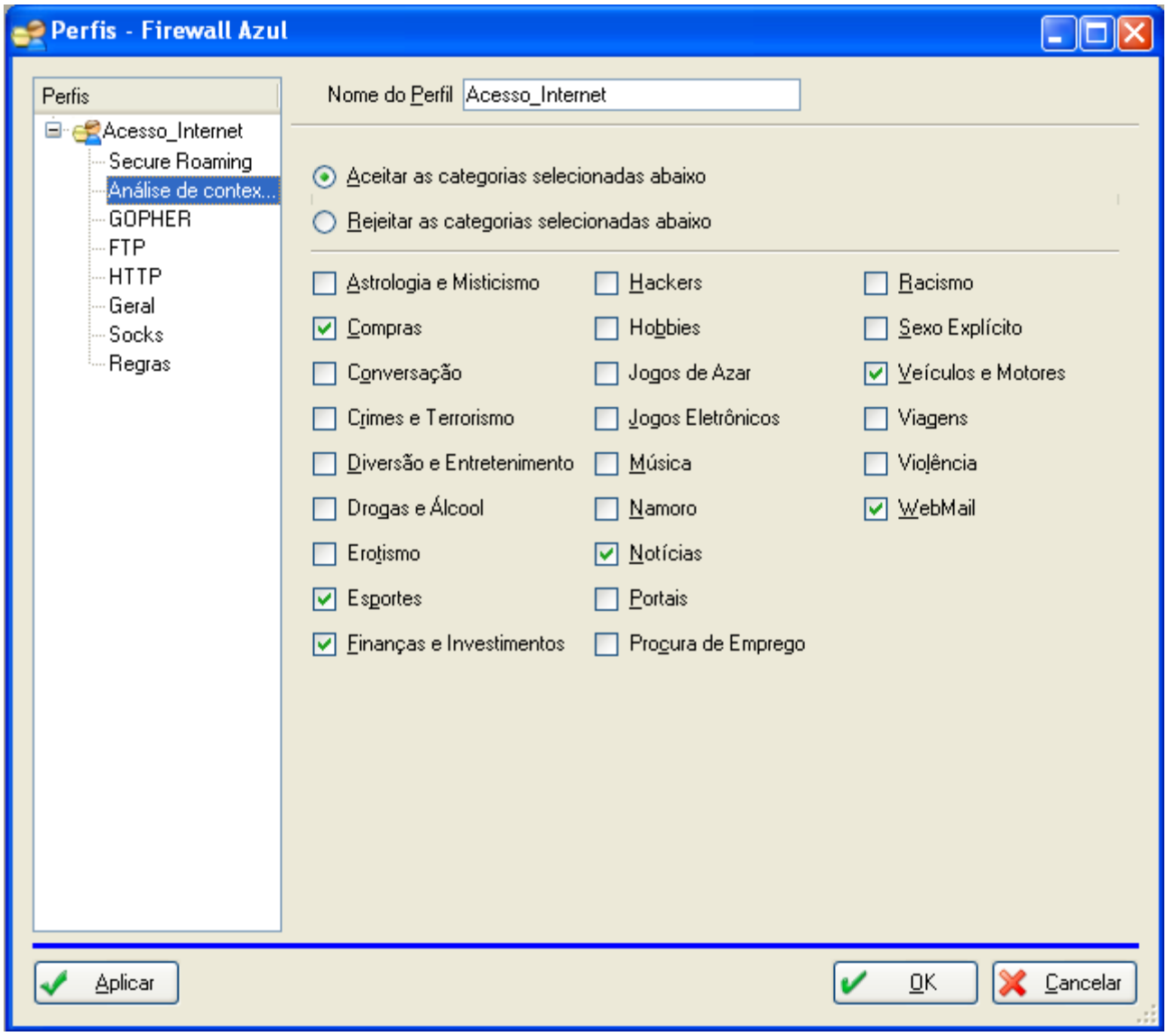
Dica: A posição de cada regra pode ser alterada, bastando clicar e arrastar a mesma para a nova posição desejada, soltando em seguida. Observe que o cursor de indicação do mouse irá mudar para uma mão segurando um bastão.

A ordem das regras na lista de regras de filtragem WWW é de fundamental importância. Ao receber uma solicitação de acesso a um endereço, o firewall pesquisará a lista a partir do início, procurando por uma regra na qual o endereço se encaixe. Tão logo uma seja encontrada, a ação associada a ela será executada.

Cada regra de filtragem consiste de uma operação, que indica que tipo de pesquisa será feita e, o texto a ser pesquisado. As seguintes opções operação estão disponíveis:

- **CONTÉM:** A URL deve conter o texto informado em qualquer posição.
- **NÃO CONTÉM:** A URL não pode conter o texto informado.
- **É:** O conteúdo da URL deve ser exatamente igual ao texto informado.
- **NÃO É:** O conteúdo da URL deve ser diferente do texto informado.
- **COMEÇA COM:** O conteúdo da URL deve começar com o texto informado.
- **NÃO COMEÇA COM:** O conteúdo da URL não pode começar com o texto informado.
- **TERMINA COM:** O conteúdo da URL deve terminar com o texto informado.
- **NÃO TERMINA COM:** O conteúdo da URL não pode terminar com o texto informado.
- **Expressão Regular:** O campo a ser pesquisado deverá ser uma expressão regular.

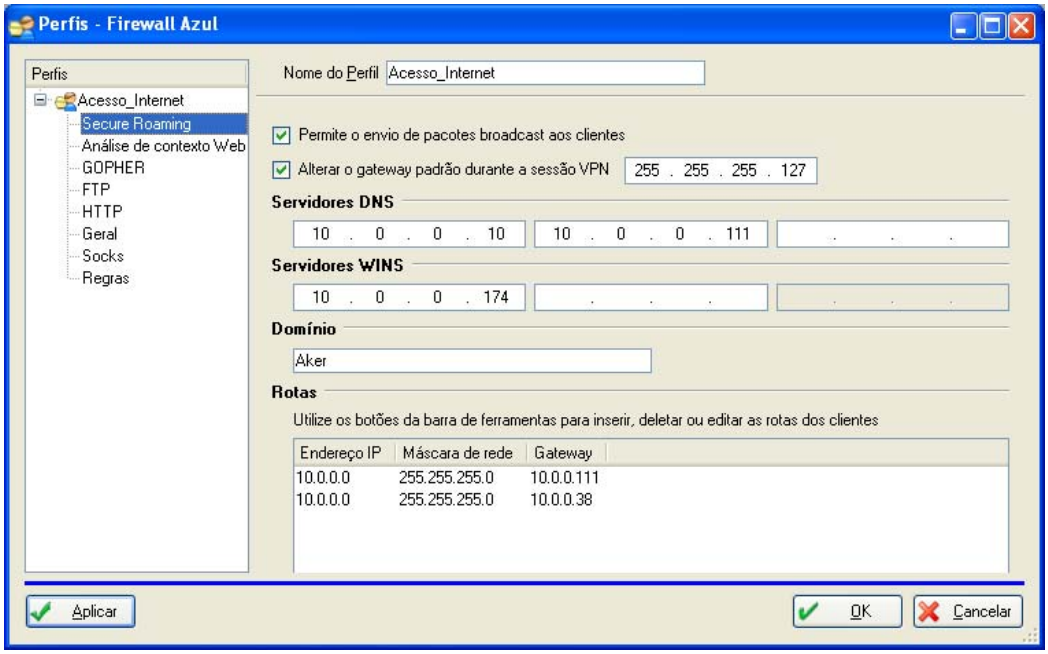
Análise de contexto Web



Essa pasta somente é útil caso se esteja utilizando o Analisador de URLS Aker. Ela permite que se especifique quais categorias poderão ou não ser visualizadas pelo usuário.

Caso a opção **Aceita categorias selecionadas** esteja marcada então o firewall permitirá que um usuário acesse a URL desejada apenas se ela pertencer a uma das categorias marcadas. Caso contrário, ou seja, se a opção **Não aceita categorias selecionadas** estiver marcada então o firewall permitirá que um usuário acesse a URL desejada apenas se ela não pertencer a nenhuma das categorias marcadas.

Secure Roaming



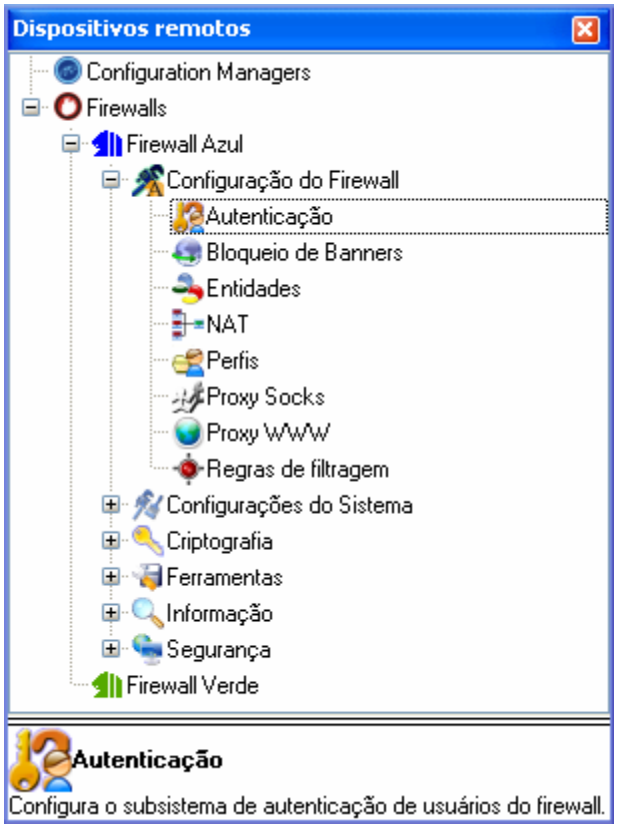
Essa pasta permite que se configurem as opções de acesso do Secure Roaming que variam de acordo com as permissões do cliente que está conectado. Para as demais configurações, veja o capítulo Configurações do Secure Roaming.

- **Permite o envio de pacotes broadcast aos clientes:** Pacotes broadcast são utilizados por protocolos que precisam, em algum ponto de seu funcionamento, uma comunicação entre um hosts e todos os outros de uma sub-rede de modo eficiente. Esse é o caso do protocolo Netbios sobre IP. Infelizemente, o abuso no uso desse tipo de pacote pode causar o congestinamento de um link lento, como uma conexão dial-up.
- **Alterar o gateway padrão durante a sessão VPN:** Ao se alterar a rota padrão dos hosts que se conectam via Secure Roaming, eles passam a não conseguir acessar outros destinos na Internet sem passar por dentro da rede com os endereços virtuais do Secure Roaming. Isso significa que, para conexões bidirecionais, eles ficam protegidos pelo firewall coorporativo e também seujeitos às políticas nele definidas.
- **Servidores DNS:**configura até três servidores DNS a serem usados durante a sessão criptográfica. Usado para o caso de haver um servidor de DNS interno na coorporação.
- **Servidores WINS:** configura até três servidores WINS a serem usados durante a sessão criptográfica. Da mesma forma, essa configuração será útil no caso de a coorporação usar servidores WINS internos. É ignorada pelos clientes Linux e FreeBSD.
- **Domínio:** Acrescenta um domínio às configurações de nomes da máquina cliente durante a sessão criptográfica. Geralmente usado em conjunto com a alteração dos servidores DNS.
- **Rotas:** Durante a sessão do cliente, algumas rotas podem ser necessárias para acessar diversos serviços da rede interna. Elas se cadastram uma a uma nesse campo.

20-3 Associando Usuários com Perfis de Acesso

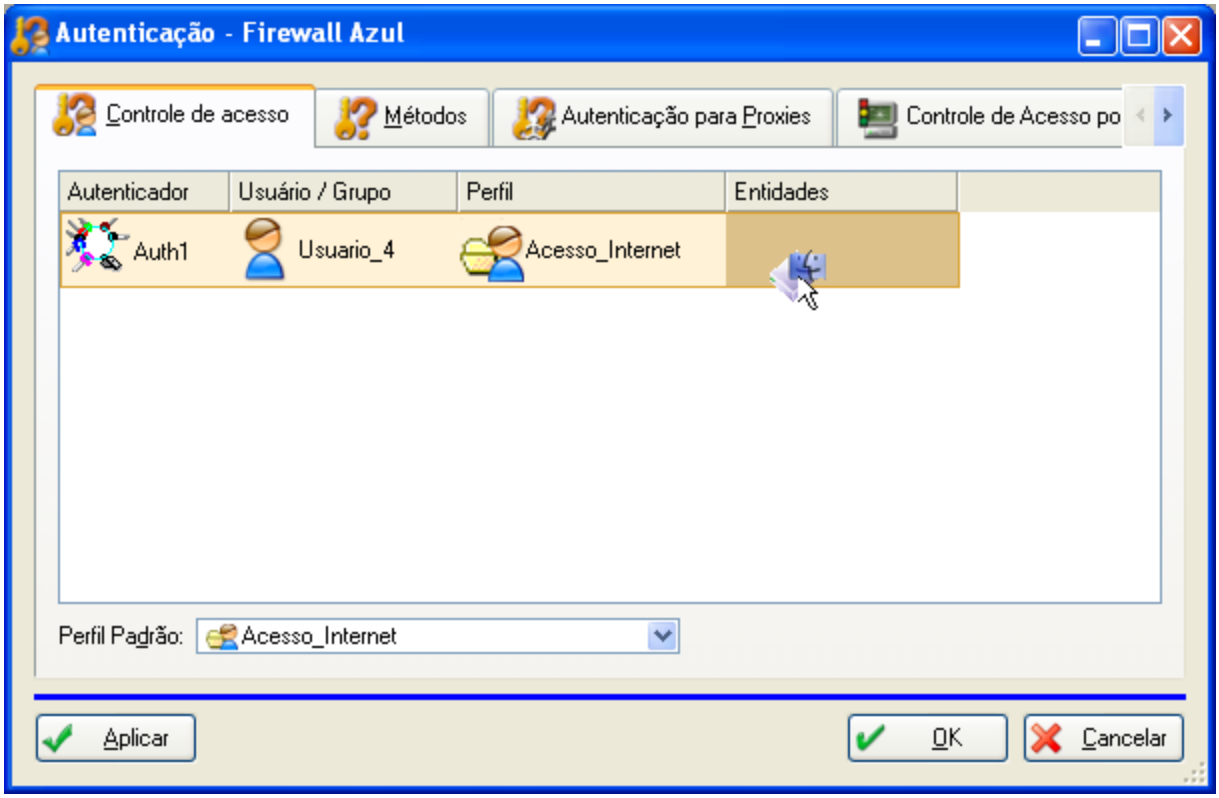
Uma vez que os perfis de acesso estão criados, é necessário associá-los com usuários e grupos de um ou mais autenticadores ou autoridades certificadoras do firewall. Isto é feito através da janela de controle de acesso.

Para ter acesso a janela de controle de acesso basta:



- Clicar no menu *Configurações* da janela principal
- Selecionar o item *Autenticação*
- Selecionar a pasta *Controle de Acesso*

A pasta de Controle de Acesso



A janela de controle de acesso permite que seja criada a associação de usuários/grupos com um perfis de acesso.

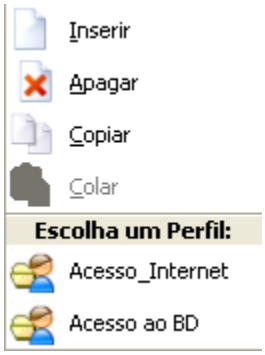
Na parte inferior da janela existe um campo chamado **Perfil Padrão** onde se pode selecionar o perfil que será associados a usuários que não se enquadrem em nenhuma regra de associação.

A última coluna, quando preenchida, especifica redes e máquinas onde a associação é válida. Se o usuário se encaixar na regra, mas estiver em um endereço IP fora das redes e máquinas cadastradas, então a regra será pulada, permitindo a atribuição de outro perfil ao usuário. Esse tipo de restrição é muito útil para permitir acesso à áreas sensíveis da rede apenas de alguns locais físicos com segurança aumentada.

Para se associar um usuário ou grupo com um determinado perfil de acesso, deve-se proceder da seguinte maneira:

1. Clica-se com o botão direito do mouse na lista de regras e seleciona-se a opção **Inserir**
2. Seleciona-se o autenticador do qual se deseja obter a lista de usuários ou grupos, clicando-se com o botão direito no campo *Autenticador*. Para maiores informações sobre os autenticadores, veja o capítulo intitulado Configurando parâmetros de autenticação).
3. Clica-se com o botão direito sobre o campo *Usuário/Grupo* e seleciona-se entre listagem de usuários ou grupos e sua lista será montada automaticamente a partir do autenticador selecionado. A partir da lista seleciona-se o usuário ou grupo desejado.

4. Clica-se com o botão direito sobre o campo *Perfil* para se selecionar o perfil desejado, conforme o menu abaixo:



5. Se desejar, arraste algumas entidades máquina, rede ou conjuntos para o campo entidades. Se o usuário estiver fora dessas entidades, a regra será pulada.

Para se remover uma regra entre um usuário/grupo e um perfil, deve-se proceder da seguinte maneira:

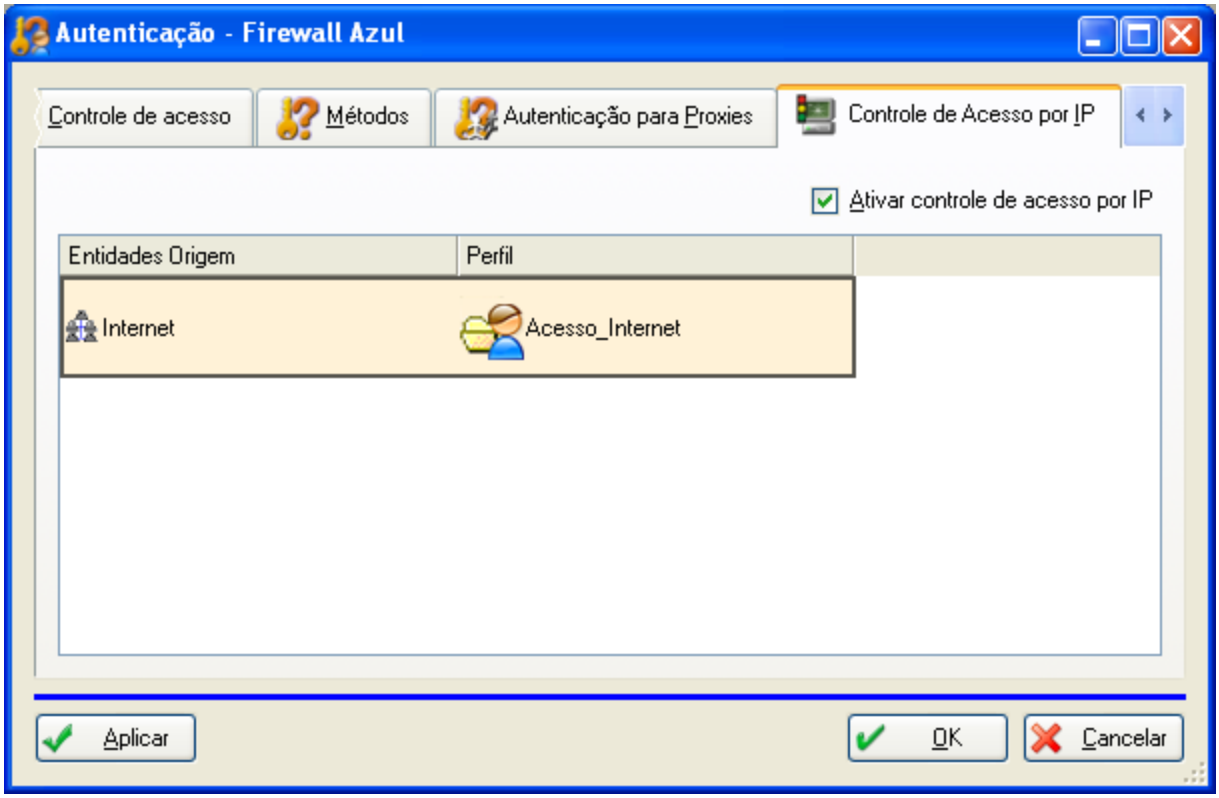
1. Clica-se na regra a ser removida, na lista da janela.
2. Clica-se no botão **Apagar**.

Para se alterar a posição de uma regra dentro da lista, deve-se proceder da seguinte forma:

1. Clica-se na regra a ser movida de posição
2. Arrasta-se para a posição desejada.

A ordem das associações na lista é de fundamental importância. Quando um usuário se autenticar, o firewall pesquisará a lista a partir do início procurando pelo nome desse usuário ou por um grupo de que ele faça parte. Tão logo um desses seja encontrado, o perfil associado ao mesmo será utilizado.

A janela de Controle de Acesso por IP



O firewall pode controlar os acessos por intermédio de endereços IP conhecidos juntamente com perfis criados para este fim. Basta o administrador cadastrar a rede conhecida e arrastar para a posição *Entidades de Origem*, em seguida incluir na coluna *Perfil* o perfil ou perfis necessários na regra.

A caixa **Ativar controle de acesso por endereço IP origem** deverá estar marcada para que o firewall use esta facilidade.

21-0 O Cliente de Autenticação Aker

Mostraremos aqui o que é e para que serve o Cliente de Autenticação Aker, uma ferramenta que propicia grande nível de segurança.

21-1 Planejando a instalação.

O que é o Cliente de Autenticação Aker ?

No capítulo anterior, mostrou-se o que são perfis de acesso de usuários, quais as facilidades que eles proporcionam ao administrador do firewall e como associar usuários de autenticadores do firewall com perfis de acesso. Entretanto, em nenhum momento foi mostrado como o firewall iria detectar que um usuário específico estaria utilizando uma máquina em um determinado momento.

Para possibilitar que o firewall saiba exatamente que usuários estão utilizando quais máquinas, existe um programa chamado Cliente de Autenticação Aker, que deve ser instalado em todas as máquinas nas quais se pretende utilizar controle de acesso por usuário. Este programa, que funciona de forma totalmente transparente para os usuários finais, intercepta o logon destes usuários no domínio, ou solicita uma nova autenticação caso se esteja utilizando autenticação por token ou smart cards, e envia esses dados, de forma criptografada, para o firewall. O firewall então valida os dados recebidos utilizando seus agentes de autenticação, autenticadores token ou autoridades certificadoras e, caso o usuário tenha sido validado corretamente, estabelece uma sessão para o usuário validado a partir da máquina na qual ele estabeleceu a sessão.

A partir deste momento, o usuário terá seu perfil de acesso configurado e terá acesso a todos os serviços liberados para ele. Quando ele efetuar logoff, o cliente de autenticação detectará este fato e informará ao firewall que o usuário finalizou sua sessão. Novamente, tudo é feito de forma transparente e automática.

O cliente de autenticação utilizará a porta 1022/UDP (serviço Aker-CL) para se comunicar com os firewalls com os quais ele estabelecerá as sessões de usuários. É necessário que exista pelo menos uma regra de filtragem liberando o acesso a partir das máquinas com o cliente instalado para o firewall, caso contrário não será possível o estabelecimento das sessões.

O cliente de autenticação não funciona através de conversão de endereços, ou seja, não é possível para uma máquina atrás de um firewall que realiza conversão de endereços estabelecer uma sessão com um firewall localizado no lado externo da conversão.

21-2 Instalando o Cliente de Autenticação Aker

O Cliente de Autenticação Aker funciona em plataformas Windows 9*/NT/2000/XP. Sua instalação é bastante simples, entretanto será necessário reinicializar a máquina após a instalação para iniciar o cliente.

Para instalar o cliente de criptografia deve-se colocar o CD-ROM no drive e selecionar a opção **Instalar Cliente de Autenticação**, dentro do menu **Firewall**, na janela de apresentação. Caso a opção de auto-execução esteja desabilitada, então é necessário se executar os seguintes passos:

1. Clicar no menu **Iniciar**
2. Selecionar a opção **Executar**
3. Ao ser perguntado sobre qual programa executar, selecione a pasta **`D:\br\firewall\auth`** e execute o único arquivo presente (Caso o leitor de CD-ROM seja acessado por uma letra diferente de D, substituí-la pela letra equivalente, no comando anterior).

A janela de instalação será mostrada. Para prosseguir, siga as instruções apresentadas na tela.

Ao término da instalação, será criado um grupo chamado **Firewall Aker**, no menu **Iniciar**. Dentro deste grupo será criado um novo grupo chamado de **Cliente de Autenticação**. Para se executar a configuração do cliente de autenticação, basta selecionar a opção **Configurar Cliente de Autenticação**, dentro deste grupo.

Instalando o cliente através de scripts

Para facilitar a instalação do Cliente de Autenticação Aker em um grande número de máquinas, é possível automatizá-la e realizá-la de forma não interativa. Com isso, pode-se escrever um script de logon, por exemplo, que instale o cliente caso ele já não esteja instalado.

A instalação automática, não interativa, é acionada através de um outro programa, chamado de **`Setupbat`**, localizado no mesmo diretório do programa de instalação descrito acima. Ele recebe as opções de instalação através da linha de comando, sendo que as seguintes opções estão disponíveis:

`-a`	Executa instalação automática
`-d` ***`diretório`***	Especifica diretório de instalação
`-f`	Instala cliente mesmo se já detectar uma instalação anterior
`-e`	Instala cliente sem a interface de configuração

Caso não se tenha especificado a opção **`-d diretório`**, o cliente será instalado em **`C:\Arquivos de Programas\aker\aker_authenticator`**

Cao a opção **-e** tenha sido especificada, é necessário se criar um arquivo de configuração para ser distribuído junto com o cliente, já que não será possível configurá-lo através da interface gráfica. Os procedimentos de criação desse arquivo estão descritos abaixo.

Distribuindo uma configuração padrão na instalação do cliente

Além de instalar o cliente automaticamente, é possível também distribuir uma configuração padrão, que será utilizada tanto na instalação automática quanto na interativa. Desta forma, o administrador de um firewall pode deixar toda a configuração do Cliente de Autenticação Aker pronta, de forma que os usuários finais não necessitem de realizar qualquer tipo de configuração.

Para instalar o cliente com uma configuração padrão, basta se configurá-lo em uma máquina, da forma desejada, e a seguir copiar um arquivo para o diretório de onde as versões padronizadas serão instaladas. O programa de instalação detectará que o arquivo existe e automaticamente os copiará para o diretório onde o programa será instalado.

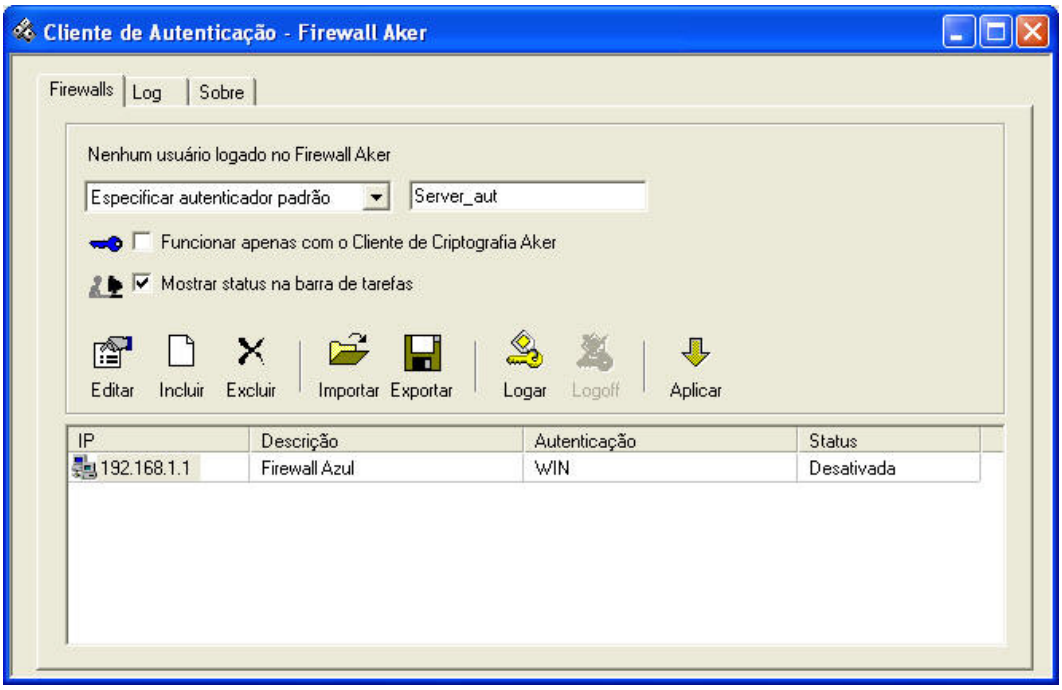
O seguinte arquivo pode ser copiado:

firewalls.clp	Lista de firewalls nos quais o cliente tentará efetuar o logon

21-3 Configurando o Cliente de Autenticação

O Cliente de Autenticação Aker roda sempre em segundo plano. Para configurá-lo é necessário executar o programa de configuração, descrito no na seção acima.
O programa de configuração consiste de 3 pastas, cada uma responsável por uma tarefa distinta. São elas:

Firewalls



Esta é a pasta principal da configuração do cliente. Ela consiste de uma lista onde são mostradas todos os firewalls nos quais o cliente tentará estabelecer uma sessão. Para cada firewall existe uma coluna indicando que métodos de autenticação podem ser utilizados e uma coluna de status indicando se existe uma sessão estabelecida ou não.

Para se incluir um novo firewall na lista, basta se clicar no botão **Incluir**, localizado na barra de ferramentas. Para se remover ou editar um firewall, basta se selecionar o firewall a ser removido ou editado e clicar na opção correspondente da barra de ferramentas.

No caso das opções *Incluir* ou *Editar* será mostrada seguinte janela:

IP: É o endereço IP do firewall para o qual o cliente tentará estabelecer uma sessão.

Descrição: É um campo livre, utilizado apenas para fins de documentação.

Autenticar apenas após acessar rede dial-up: Se essa opção estiver marcada o cliente de autenticação tentará estabelecer uma sessão com o firewall apenas após uma sessão dial-up for estabelecida. Essa opção é particularmente útil para clientes instalados em laptops.

Métodos de autenticação suportados: Esse campo indica quais métodos de autenticação serão utilizados para validar um usuário para o firewall. Ele consiste das seguintes opções:

Windows logon: Se essa opção estiver marcada, o cliente de autenticação capturará o nome e a senha do usuário que se logou no Windows e os utilizará para estabelecer a sessão com o firewall. Nesse caso, a autenticação será totalmente transparente, ou seja, não será mostrada nenhuma nova tela para o usuário.

Usuário e senha: Se essa opção estiver marcada, será mostrada uma tela para o usuário a fim de que seja informado um nome e uma senha para o estabelecimento da sessão com o firewall.

SecurID: Se essa opção estiver marcada, será mostrada uma tela para o usuário a fim de que seja informado um nome, um PIN e o código do token para o estabelecimento da sessão com o firewall.

Smart Card: Se essa opção estiver marcada, será mostrada uma tela para o usuário a fim de que seja informado o PIN do seu smart card para o estabelecimento da sessão com o firewall.

Caso mais de uma opção esteja selecionada (exceto a de Windows Logon), será mostrada uma tela onde o usuário tem a possibilidade de escolher o método de autenticação desejado a cada nova sessão.

Caso se tenha escolhido autenticação por smart cards e não exista um leitor de smart cards na máquina, essa opção será ignorada.

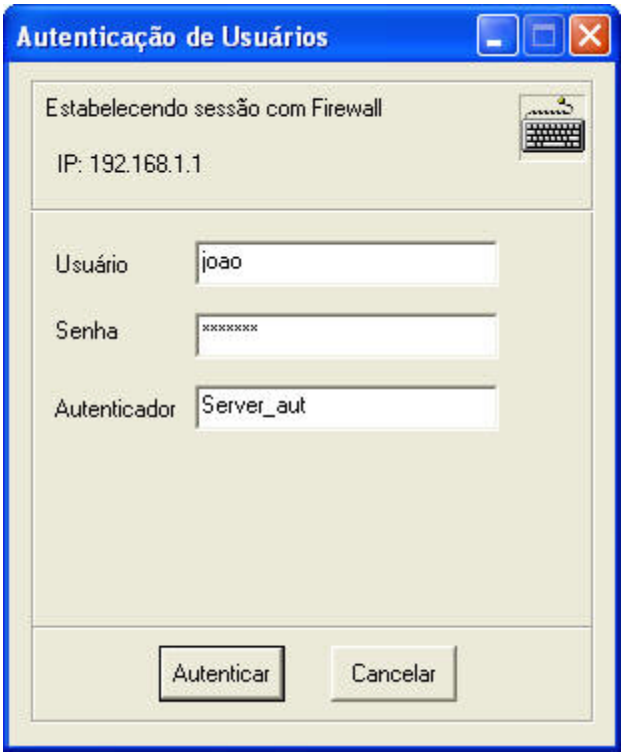
É possível se exportar a configuração atual para um arquivo e importá-la posteriormente na mesma ou em outra máquina. Para tal, existem os botões **Importar** e **Exportar**, localizados na barra de ferramentas. O botão **Importar** salva a lista de firewalls e as demais opções da janela em um arquivo e o botão **Exportar** carrega uma lista de firewalls e as demais opções a partir de um arquivo e acrescenta os firewalls na lista atual (as novas entradas serão acrescentadas ao final da lista atual).

O botão **Logoff** faz com que o cliente encerre a sessão com o firewall selecionado. Ele só estará habilitado caso se tenha selecionado um firewall com o qual exista uma sessão ativa.

O botão **Logar** faz com que o cliente tente estabelecer uma sessão com o firewall selecionado. Ele só estará habilitado caso se tenha selecionado um firewall com o qual

ainda não exista uma sessão ativa. Ao ser clicado, ele mostrará uma das janelas abaixo, a depender do tipo de autenticação selecionado:

- **Autenticação por usuário/senha**



Usuário: É o nome do usuário que deseja estabelecer a sessão.

Senha: É a senha do usuário que deseja estabelecer a sessão

Autenticador: É o nome do autenticador no qual o usuário se deseja autenticar. Este campo pode ser deixado em branco. Para maiores informações sobre os autenticadores, veja o capítulo entitulado Configurando parâmetros de autenticação.

- **Autenticação por Token (SecurID)**

Usuário: É o nome do usuário que deseja estabelecer a sessão.

PassCode: É a combinação do PIN do usuário seguido pelo número mostrado no token SecurID

- **Autenticação por Smart Card**

No caso de autenticação por Smart Cards, a tela mostrada será dependente do tipo de smart card que se está utilizando. A mostrada acima é apenas uma das possibilidades.

O botão **Aplicar** serve para que as alterações recém feitas sejam salvas se tornem permanentes. Ao ser clicado, todas as sessões que por ventura estejam ativas serão derrubadas.

Na parte superior da pasta, existe um campo que permite com que se especifique a forma com que o cliente de autenticação vai lidar com os autenticadores. Essa opção só é utilizada no caso de autenticação por *Windows Logon* e consiste de três opções:

Não especificar autenticador: Esta opção informa ao cliente para ele enviar o campo autenticador em branco, quando for efetuar um logon em um firewall. Desta forma, o firewall irá pesquisar sua lista de autenticadores normalmente.

Usar domínio NT como autenticador: Esta opção informa ao cliente para enviar o nome do domínio NT como nome do autenticador para o firewall, fazendo com que o firewall utilize este autenticador para validar o usuário. Para que esta opção funcione, é necessário que exista um autenticador ativo com o nome do domínio NT utilizado e que o firewall esteja configurado para permitir que os usuários especifiquem um domínio. Para maiores informações sobre estes parâmetros, veja o capítulo entitulado Configurando parâmetros de autenticação.

Especificar Autenticador Padrão: Esta opção permite ao usuário especificar o nome de um autenticador que será utilizado pelo cliente ao efetuar logon no firewall. Para que esta opção funcione, é necessário que exista um autenticador ativo com o nome

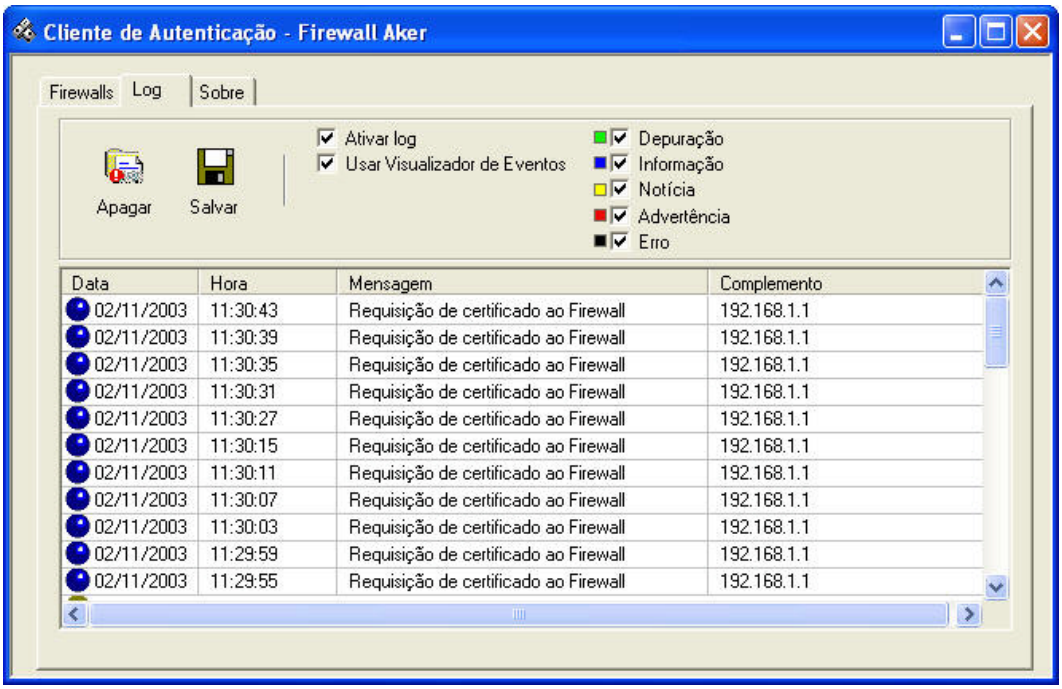
especificado e que o firewall esteja configurado para permitir que os usuários especifiquem um domínio. Para maiores informações sobre estes parâmetros, veja o capítulo entitulado Configurando parâmetros de autenticação.

A opção **Funcionar Apenas com o Cliente de Criptografia Aker,** se estiver marcada, faz com que o cliente de autenticação somente tente estabelecer uma sessão com um firewall se o cliente de criptografia estiver ativo. Isso serve para se acrescentar um grau se segurança ainda maior, já que o cliente de criptografia utiliza certificados assinados e, com isso, consegue validar o firewall com o qual ele está se comunicando.

Toda a comunicação entre o Cliente de Autenticação Aker e os firewalls é criptografada, mesmo se a opção **Funcionar Apenas com o Cliente de Criptografia Aker** estiver desmarcada. A única segurança a mais acrescentada pelo cliente de criptografia é o fato deste validar, através de certificados digitais assinados, que o firewall com o qual se está comunicando é realmente o firewall verdadeiro, impedindo ataques do tipo *men-in-the-middle*.

A opção **Mostrar status na barra de tarefas**, se estiver marcada, faz com que seja mostrado um ícone na barra de tarefas da área de trabalho que permite se verificar se existe ou não uma sessão estabelecida.

Log


Cliente de Autenticação - Firewall Aker
Firewalls
Log
Sobre
Apagar
Salvar
Ativar log
Usar Visualizador de Eventos
Depuração
Informação
Notícia
Advertência
Erro
Data
Hora
Mensagem
Complemento
02/11/2003 11:30:43 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:30:39 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:30:35 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:30:31 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:30:27 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:30:15 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:30:11 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:30:07 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:30:03 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:29:59 Requisição de certificado ao Firewall 192.168.1.1
02/11/2003 11:29:55 Requisição de certificado ao Firewall 192.168.1.1

Esta pasta é muito útil para se acompanhar o funcionamento do cliente de autenticação. Ela consiste de uma lista com diversas mensagens ordenadas pela hora. Ao lado de cada mensagem existe um ícone colorido, simbolizando sua prioridade. As cores tem o seguinte significado:

Verde	Depuração
Azul	Informação

Amarelo	Notícia
Vermelho	Advertência
Preto	Erro

O botão **Apagar**, localizado na barra de ferramentas permite com que se apague todas as entradas existentes no log.

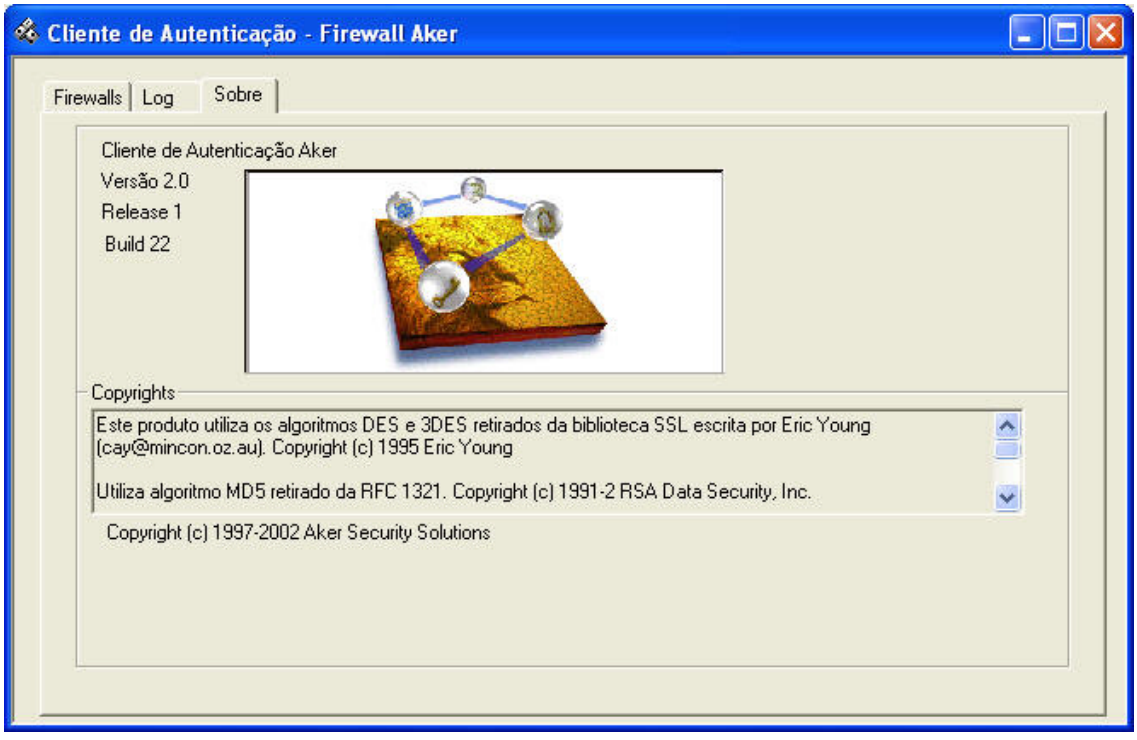
O botão **Salvar**, localizado na barra de ferramentas permite com que se salve o log em um arquivo formato texto. Ao ser clicado, será mostrada uma janela para que se especifique o nome do arquivo que será salvo.

A opção **Ativar Log**, se estiver desmarcada, fará com que novas entradas de log não sejam mais geradas pelo cliente de autenticação.

A opção **Usar visualizador de eventos**, se estiver marcada fará com que todas as mensagens de log sejam enviadas para o Visualizador de eventos do Windows

O log do Cliente de Autenticação Aker é armazenado apenas durante a execução do cliente. Caso a máquina seja reinicializada, todas as suas informações serão descartadas.

Sobre

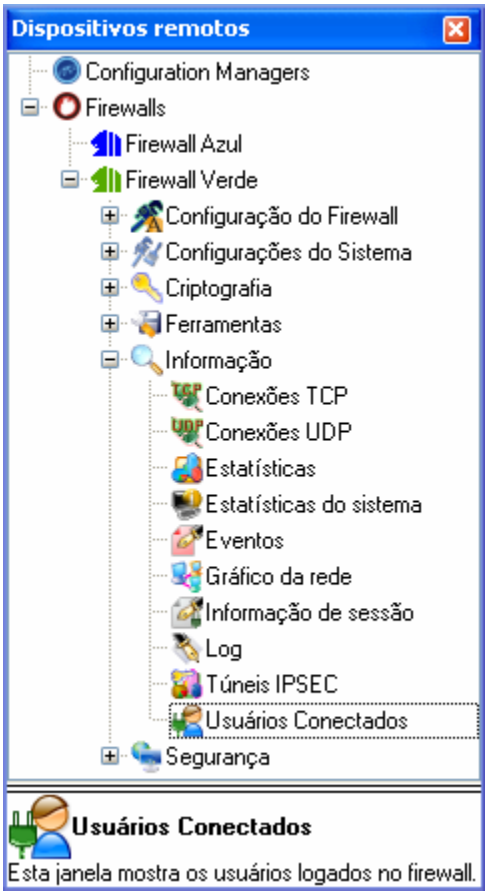

Cliente de Autenticação - Firewall Aker
Firewalls
Log
Sobre
Cliente de Autenticação Aker
Versão 2.0
Release 1
Build 22
Copyrights
Este produto utiliza os algoritmos DES e 3DES retirados da biblioteca SSL escrita por Eric Young (cay@mincon.oz.au). Copyright (c) 1995 Eric Young
Utiliza algoritmo MD5 retirado da RFC 1321. Copyright (c) 1991-2 RSA Data Security, Inc.
Copyright (c) 1997-2002 Aker Security Solutions

Esta é uma pasta meramente informativa e serve para que se obtenha algumas informações do cliente. Dentre as informações úteis se encontram sua versão e release.

21-4 Visualizando e Removendo Usuários Logados no Firewall

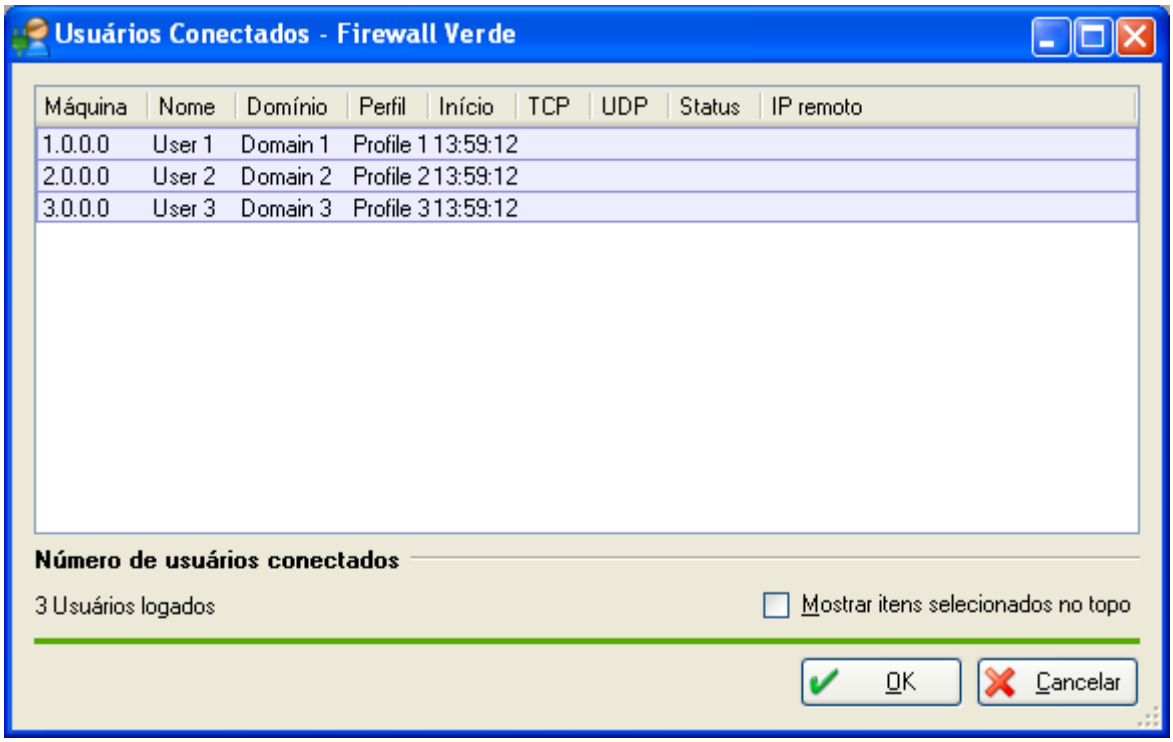
É possível se visualizar a qualquer momento os usuários que possuem sessão estabelecida com o firewall, através do cliente de autenticação, e remover uma destas sessões. Isto é feito através da janela de usuários logados.

Para ter acesso a janela de usuários logados basta:



- Clicar no menu *Informação* da janela de administração do firewall
- Selecionar *Usuários Conectados*

A janela de Usuários Conectados



Esta janela consiste de uma lista com uma entrada para cada usuário. Na parte inferior da janela é mostrada uma mensagem informando o número total de usuários com sessões estabelecidas um determinado instante. Para os usuários logados via Secure Roaming, serão mostrados também os dados da conexão (endereço IP e portas) junto com o estado de estabelecimento da mesma.

- O botão **OK** faz com que a janela de usuários seja fechada.
- O botão **Cancelar** fecha a janela
- A caixa **Itens selecionados no topo** coloca os itens que foram selecionados para o topo da janela de usuários conectados.

Barra de Ferramentas de Usuários Conectados

- O botão **Atualizar** faz com que as informações mostradas sejam atualizadas periodicamente de forma automática ou não. Clicando-se sobre ele, alterna-se entre os dois modos de operação. O intervalo de atualização pode ser configurado mudando-se o valor logo a direita deste campo.
- O botão **Remover**, localizado na barra de ferramentas, permite que se remova uma sessão de usuário. Para tal deve-se primeiro clicar sobre a sessão que se deseja remover e a seguir clicar neste botão (ele estará desabilitado enquanto não existir nenhuma sessão selecionada).
- O botão **DNS**, localizado na barra de ferramentas, acionará o serviço de nomes (DNS) para resolver os nomes das máquinas cujos endereços IPs aparecem listados. Cabem ser observados os seguintes pontos:

1. A resolução de nomes muitas vezes é um serviço lento e, devido a isso, a tradução dos nomes é feita em segundo plano.
2. Muitas vezes, devido a problemas de configuração do DNS reverso (que é o utilizado para resolver nomes a partir de endereços IP), não será possível a resolução de certos endereços. Neste caso, os endereços não resolvidos serão mantidos na forma original e será indicado ao seu lado que eles não possuem DNS reverso configurado.

- É possível se ordenar a lista das sessões por qualquer um de seus campos, bastanto para isso clicar no título do campo. O primeiro click produzirá uma ordenação ascendente e o segundo uma ordenação descendente.

Significado dos campos de uma sessão de usuário ativa

Cada linha presente na lista de sessões de usuários representa uma sessão. O significado de seus campos é o seguinte:

Ícone: É mostrado a esquerda do nome de cada usuário e pode assumir três formas distintas:

Cadeado: Este ícone indica que o usuário se logou através do cliente de criptografia apenas

Usuário: Este ícone indica que o usuário se logou através do cliente de autenticação apenas

Usuário dentro do cadeado: Este ícone indica que o usuário se logou através do cliente de autenticação e de criptografia

Máquina: Endereço IP ou nome (caso o DNS esteja ativo) da máquina na qual a sessão foi estabelecida.

Nome: Nome do usuário que estabeleceu a sessão

Domínio: Nome do domínio, i.e. autenticador, no qual o usuário se autenticou. Caso o usuário não tenha especificado domínio ao se logar, este campo aparecerá em branco

Perfil: Qual o perfil de acesso correspondente a esta sessão. Se este campo está em branco, o usuário se autenticou antes de a tabela de perfis ser alterada, de forma que ele está utilizando um perfil que não existe mais.

Início: Hora de abertura da sessão.

21-5 Utilizando a Interface Texto

A interface texto para acesso à lista de usuários logados possui as mesmas capacidades da interface gráfica e é simples de ser utilizado. Ele é o mesmo programa que produz a lista de conexoes ativas TCP e UDP, mostrado anteriormente.

Localização do programa: `/etc/firewall/fwlist`

Sintaxe:

```
Uso: fwlist ajuda
     fwlist mostra [[-w] [TCP]] | [UDP] | [sessoes]
     fwlist remove [TCP | UDP] IP_origem Porta_origem IP_destino
Porta_destino
     fwlist remove sessao IP_origem
```

Ajuda do programa:

```
Firewall Aker - Versao 5.0
fwlist - Lista e remove conexoes TCP/UDP e sessoes ativas
Uso: fwlist ajuda
     fwlist mostra [[-w] [TCP]] | [UDP] | [sessoes]
     fwlist remove [TCP | UDP] IP_origem Porta_origem IP_destino
Porta_destino
     fwlist remove sessao IP_origem

     ajuda  = mostra esta mensagem
     mostra = lista as conexoes ou sessoes ativas
     remove = remove uma conexao ou sessao ativa
```

Exemplo 1: (listando as sessões de usuários logados no firewall)

```
#fwlist mostra sessoes
Nome/Dominio                          Perfil           IP origem
Inicio
------------------------------------------------------------------------
---------
administrador/BSB                     Admin            10.20.1.1
08:11:27
jose.silva/GOA                        Padrao5          10.45.1.1
07:39:54
joao.souza/POA                        Padrao3          10.57.1.1
07:58:10
josemaria/GRU                         Padrao3          10.78.1.1
08:01:02
angelam/BSB   1                       Restrito         10.22.1.1
08:48:31
marciam/POA                           Restrito         10.235.1.1
10:49:44
antonioj/POA                          Especial         10.42.2.1
06:02:19
operador/BSB                          Padrao           10.151.2.1
20:44:34
```

Exemplo 2: (removendo a sessão do usuário logado a partir da máquina 10.19.1.1)

```
#fwlist remove sessao 10.19.1.1
A remocao da sessao foi solicitada ao servidor de usuarios
```

22-0 Configurando o proxy SMTP

Neste capítulo serão mostradas quais as funções oferecidas pelo proxy SMTP e como realizar sua configuração

O que é o proxy SMTP ?

O proxy SMTP é um programa especializado do Firewall Aker feito para trabalhar com correio eletrônico (SMTP é um anagrama para *Simple Mail Transfer Protocol*, que é o nome completo do serviço de transferência de correio eletrônico na Internet). Este proxy possibilita que sejam realizadas filtragens de e-mails baseadas em seu conteúdo ou em qualquer campo de seu cabeçalho. Ele também atua como uma barreira protegendo o servidor SMTP contra diversos tipos de ataques.

Ele é um proxy transparente (para maiores informações veja o capítulo intitulado Trabalhando com proxies), desta forma, nem o servidor nem o cliente sabem de sua existência.

Descrição de uma mensagem SMTP

Para se entender o funcionamento da filtragem de campos do proxy SMTP, é necessário algumas informações sobre as mensagens de correio eletrônico.

Uma mensagem de e-mail é formada por três partes distintas: envelope, cabeçalho e corpo. Cada uma destas partes possui um papel específico:

- **Envelope**

O envelope é chamado desta forma por ser análogo a um envelope de uma carta comum. Nele se encontram as informações do emissor e dos destinatários de uma mensagem. Para cada recipiente de um domínio diferente é gerado um novo envelope. Desta forma, um servidor SMTP recebe no envelope de uma mensagem o nome de todos os recipientes da mensagem que se encontram no seu domínio.

O envelope não é visto pelos destinatários de uma mensagem. Ele somente é usado entre os servidores SMTP.

- **Cabeçalho**

No cabeçalho da mensagem se encontram informações sobre a mensagem, como o assunto, data de emissão, nome do emissor, etc. O cabeçalho normalmente é mostrado ao destinatário da mensagem.

- **Corpo**

O corpo é composto pela mensagem propriamente dita, da forma com que foi produzida pelo emissor.

Ataques contra um servidor SMTP

Existem diversos ataques passíveis de serem realizados contra um servidor SMTP. São eles:

- **Ataques explorando *bugs* de um servidor**

Neste caso, o atacante procura utilizar um comando ou parâmetros de um comando que conhecidamente provocam falhas de segurança.
O proxy SMTP do Firewall Aker impede estes ataques na medida em que só permite a utilização de comandos considerados seguros e validando os parâmetros de todos os comandos.

- **Ataques explorando estouro de áreas de memória (*buffer overflows*)**

Estes ataques consistem em se enviar linhas de comando muito grandes, fazendo com que um servidor que não tenha sido corretamente desenvolvido apresente falhas de segurança.

O proxy SMTP do Firewall Aker impede estes ataques na medida em que limita o tamanho máximo das linhas de comando que podem ser enviadas para o servidor.

- **Ataques de relay**

Estes ataques consistem em utilizar o servidor SMTP de terceiros para enviar suas mensagens de correio eletrônico. Desta forma, utiliza-se os recursos computacionais que deveriam estar disponíveis para requisições válidas.

O proxy SMTP do Firewall Aker impede ataques de relay deste que corretamente configurado.

Utilizando o proxy SMTP

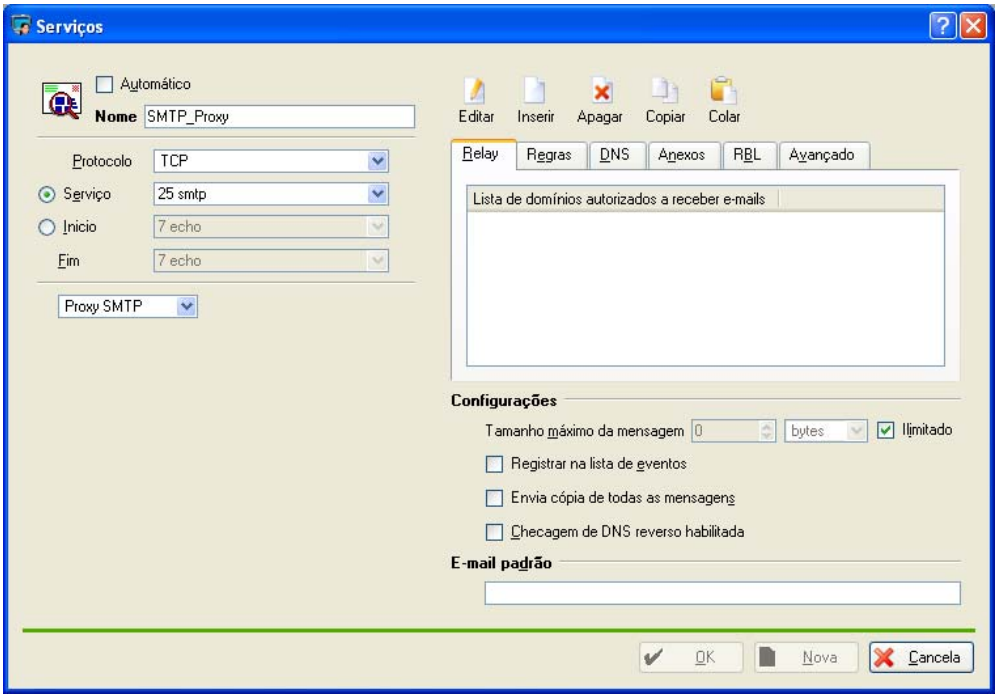
Para se utilizar o proxy SMTP em uma comunicação, é necessário se executar uma seqüência de 2 passos:

1. Cria-se um serviço que será desviado para o proxy SMTP e edita-se os parâmetros do contexto a ser usado por este serviço (para maiores informações, veja o capítulo intitulado Cadastrando Entidades)
2. Acrescenta-se uma regra de filtragem permitindo o uso do serviço criado no passo 1, para as redes ou máquinas desejadas (para maiores informações, veja o capítulo intitulado Filtro de Estados)

22-1 Editando os parâmetros de um contexto SMTP

A janela de propriedades de um contexto SMTP será mostrada quando a opção **Proxy SMTP** for selecionada. Através dela é possível se definir o comportamento do proxy SMTP quando este for lidar com o serviço em questão.

A janela de propriedades de um contexto SMTP



Na janela de propriedades são configurados todos os parâmetros de um contexto associado a um determinado serviço. Ela consiste de alguns campos comuns seguidos por seis pastas onde são configurados parâmetros específicos O campos comuns são:

Tamanho máximo da mensagem: Este campo indica o tamanho máximo, em bytes ou kbytes, de uma mensagem para que ela possa ser aceita pelo proxy. Caso não se deseje definir um tamanho máximo, basta marcar a opção **Sem Limite**, localizada à direita desta campo.

Registrar na lista de eventos: Este campo indica se as mensagens que não se enquadrarem em nenhuma regra SMTP deste contexto devem ser registradas na lista de eventos.

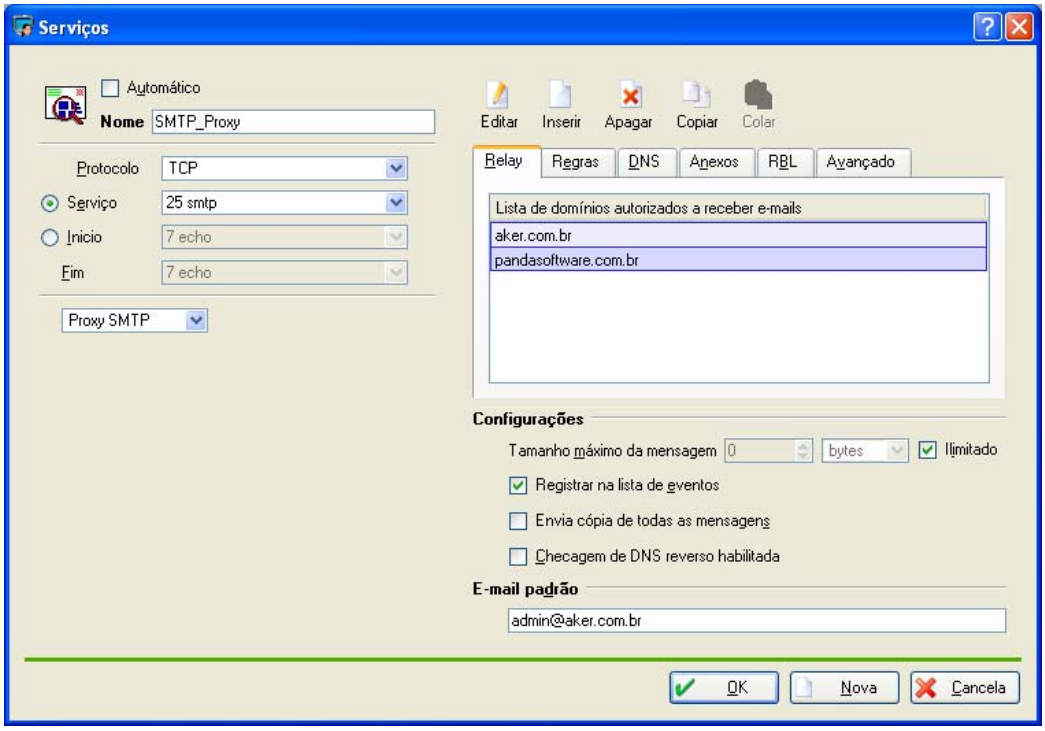
Envia cópia de todas as mensagens: Independente de uma mensagem ter sido aceita ou rejeitada, é possível se enviar uma cópia completa dela para um endereço de e-mail qualquer. Este campo indica se deve ou não ser enviada esta cópia.

Habilita checagem de DNS reverso: O firewall fará a checagem para determinar a existência do DNS reverso cadastrado para o servidor SMTP para aceitar a mensagem baseado nas regras da pasta DNS.

E-mail padrão: Indica o endereço de e-mail padrão, para o qual serão enviadas as cópias das mensagens que não se enquadrarem em nenhuma regra SMTP deste contexto

(se a opção *Envia Cópia de todas as mensagens* estiver marcada). Este e-mail também pode ser referenciado em qualquer regra de filtragem do contexto.

- **Pasta de Relay**

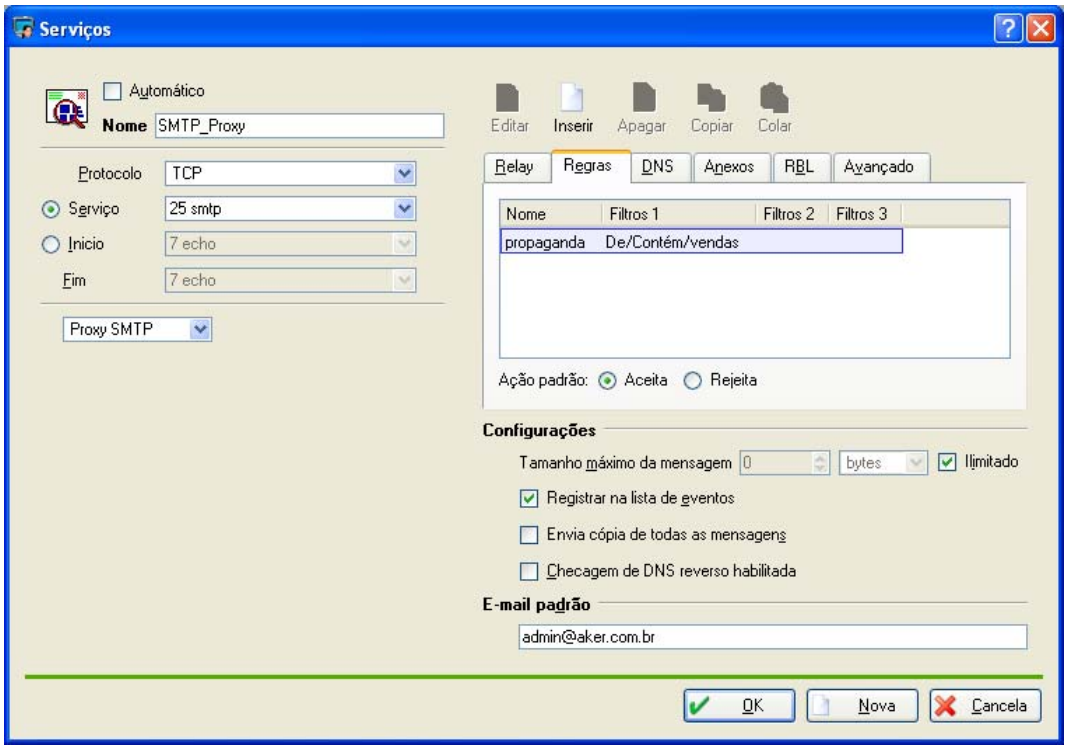


Esta pasta serve para se especificar uma lista de domínios válidos para recebimento de e-mails. E-mails destinados a quaisquer domínios não listados serão rejeitados antes mesmo que se comece sua transmissão.

Caso a lista de domínios esteja em branco o firewall não fará controle de relay, ou seja, aceitará e-mails destinados a quaisquer domínios.

Diferentemente do controle de relay de servidores SMTP, o firewall apenas pode basear seu controle no destinatário dos e-mails, e não no remetente, uma vez que não possui a lista de usuários válidos do servidor SMTP protegido.

- **Pasta de Regras**



Nesta pasta são mostradas todas as regras de filtragem para o contexto. Estas regras possibilitam que o administrador configure filtros de e-mails baseados em seu conteúdo.

Para se executar qualquer operação sobre uma determinada regra, basta clicar com o botão direito do mouse sobre ela. Aparecerá o seguinte menu: (este menu será acionado sempre que se pressionar o botão direito, mesmo que não exista nenhuma regra selecionada. Neste caso, somente as opções *Incluir* e *Colar* estarão habilitadas)

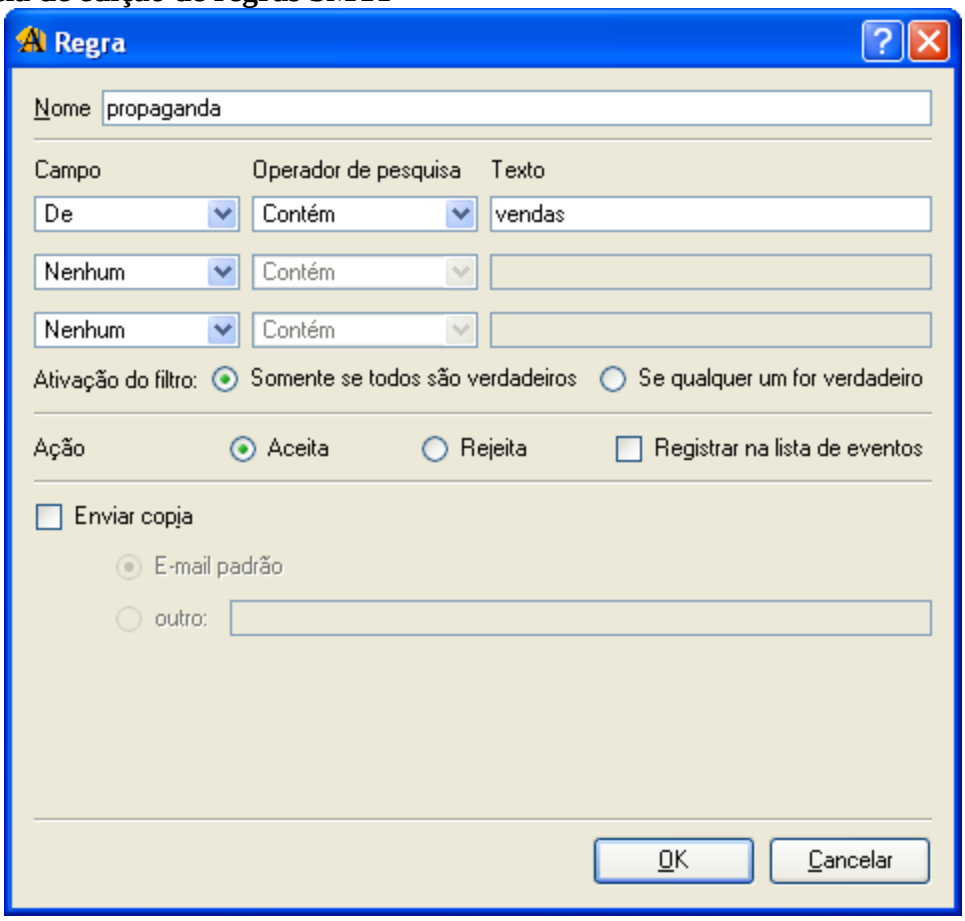
- **Inserir:** Esta opção permite se incluir uma nova regra na lista. Se alguma regra estiver selecionada, a nova será inserida na posição da regra selecionada. Caso contrário, a nova regra será incluída no final da lista.
- **Editar:** Esta opção abre a janela de edição para a regra selecionada.
- **Apagar**: Esta opção remove da lista a regra selecionada.
- **Copiar:** Esta opção copia a regra selecionada para uma área temporária.
- **Colar:** Esta opção copia a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.
- **Renomear:** Esta opção renomeia a regra selecionada da lista

Dica: Todas as opções mostradas acima podem ser executadas a partir da barra de ferramentas localizada logo acima da lista. Neste caso, primeiro seleciona-se a regra, clicando-o com o botão esquerdo, e em seguida clica-se na opção desejada.

A ordem das regras na lista de regras de filtragem SMTP é de fundamental importância. Ao receber uma mensagem, o firewall pesquisará a lista a partir do início procurando uma regra na qual a mensagem se enquadre. Tão logo uma seja encontrada, a ação associada a ela será executada.

No caso de inclusão ou edição de regras, será mostrada a janela de edição, mostrada abaixo:

A janela de edição de regras SMTP



Nesta janela são configurados todos os parâmetros relativos a uma regra de filtragem para um contexto SMTP. Cada regra consiste basicamente de 3 condições independentes que podem ou não estar preenchidas (ou seja, é possível se criar regras com apenas uma ou duas condições).

Para se criar uma regra, é necessário se preencher os seguintes campos:

Nome: Nome que define unicamente a regra dentro do contexto. Este nome será mostrado na lista de regras do contexto SMTP. Não podem existir duas regras com o mesmo nome.

Campo: Define o nome do campo dentro da mensagem SMTP onde será feita a pesquisa. Ele pode assumir um dos seguintes valores (alguns valores são mostrados em inglês devido ao fato de serem nomes de campos fixos de uma mensagem):

- **NENHUM:** Não será feita pesquisa.

- **TO (Todos):** A pesquisa é feita no endereço de destino da mensagem (todos os recipientes devem se encaixar na regra).
- **TO (Qualquer):** A pesquisa é feita no endereço de destino da mensagem (pelo menos um recipiente deve se encaixar na regra).
- **FROM:** A pesquisa é feita no endereço de origem da mensagem
- **CC:** A pesquisa é realizada sobre a lista de endereços que irão receber uma cópia da mensagem
- **REPLY:** A pesquisa é feita no campo REPLY-TO, que indica o endereço para o qual a mensagem deve ser respondida.
- **SUBJECT:** A pesquisa é feita no campo que define o assunto da mensagem
- **Cabeçalho:** A pesquisa é realizada sobre todos os campos que compõem o cabeçalho da mensagem
- **Corpo:** A pesquisa é feita no corpo da mensagem (onde existe efetivamente a mensagem).

Os campos TO e CC são tratados de forma diferente pelo proxy SMTP: o campo TO é tratado com uma lista dos vários recipientes da mensagem, retirados do envelope da mensagem. O campo CC é tratado como um texto simples, retirado do cabeçalho da mensagem, e sua utilidade é bastante limitada.

Pesquisa: Tipo de pesquisa a ser executada no campo definido acima. São elas:

- **CONTÉM:** O campo a ser pesquisado deve conter o texto informado em qualquer posição.
- **NÃO CONTÉM:** O campo a ser pesquisado não pode conter o texto informado.
- **É:** O conteúdo do campo a ser pesquisado deve ser exatamente igual ao texto informado.
- **NÃO É:** O conteúdo do campo a ser pesquisado deve ser diferente do texto informado.
- **COMEÇA COM:** O conteúdo do campo a ser pesquisado deve começar com o texto informado.
- **NÃO COMEÇA COM:** O conteúdo do campo a ser pesquisado não pode começar com o texto informado.
- **TERMINA COM:** O conteúdo do campo a ser pesquisado deve terminar com o texto informado
- **NÃO TERMINA COM:** O conteúdo do campo a ser pesquisado não pode terminar com o texto informado.
- **CONTÉM PALAVRAS:** Neste tipo de pesquisa, o texto informado é considerado como formado por palavras individuais (separadas por espaços), ao invés de um texto contínuo. Para se enquadrar na pesquisa, o campo em questão deve conter todas as palavras informadas, independente de sua posição.

Texto: Texto a ser pesquisado. Este campo é tratado como um texto contínuo que será comparado com o campo especificado, exceto no caso da pesquisa CONTÉM PALAVRAS, quando ele é tratado como diversas palavras separadas por espaços. **Em ambos os casos, letras maiúsculas e minúsculas são consideradas como sendo iguais.**

Os campos **Campo**, **Pesquisa** e **Texto** aparecem 3 vezes. Desta forma, é possível se definir até 3 condições distintas que uma mensagem deve cumprir para que seja

enquadrada pela regra. Caso não se deseje especificar três condições, basta deixar as demais com o valor NENHUM no parâmetro campo.

Ativação dos filtros: Este campo só tem sentido quando se especifica mais de uma condição. Ele indica que tipo de operação será usada para relacioná-las:

- **Somente se ambos são verdadeiros:** Para que uma mensagem se enquadre na regra, é necessário que ela satisfaça todas as condições.
- **Se qualquer um for verdadeiro:** Para que uma mensagem se enquadre na regra, basta ela satisfazer uma das condições.

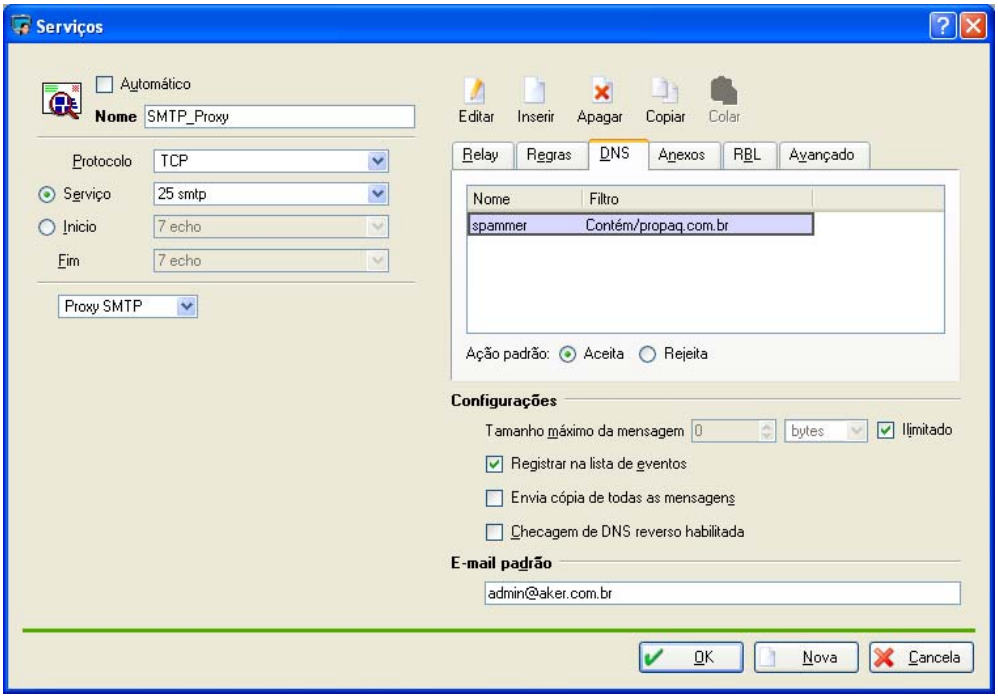
Ação: Este campo indica se as mensagens que se enquadrarem na regra devem ser aceitas ou rejeitadas pelo proxy SMTP.

Registrar na lista de eventos: Este campo indica se as mensagens que se enquadrarem na regra devem ou não ser registradas na lista de eventos.

Enviar cópia: Para toda mensagem que se enquadrar na regra, independentemente de ter sido aceita ou rejeitada, é possível se enviar uma cópia completa dela para um endereço de e-mail qualquer. Este campo indica se deve ou não ser enviada esta cópia. Caso ele esteja marcado, deve-se escolher uma das seguintes opções de envio:

- **Padrão:** A cópia da mensagem é enviada para o e-mail padrão.
- **e-mail:** A cópia da mensagem é enviada para o endereço especificado no campo à direita.

- **Pasta de DNS**



Nesta pasta são mostradas todas as regras de filtragem de DNS para o contexto. Estas regras possibilitam que o administrador configure filtros de e-mails baseados no nome retornado pelo DNS reverso do servidor SMTP que estiver enviando a mensagem.

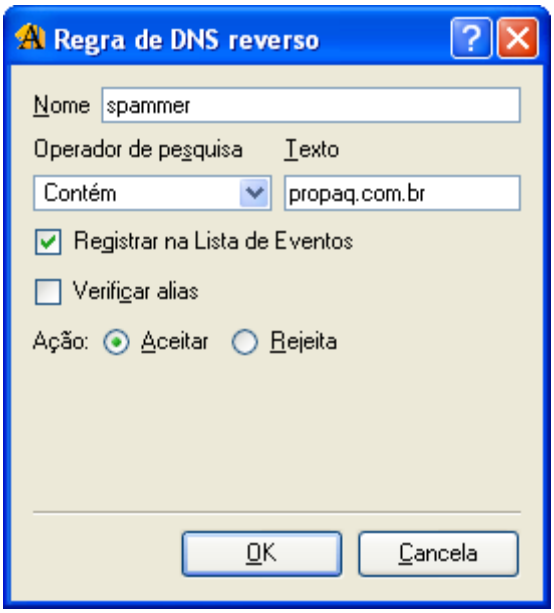
Para se executar qualquer operação sobre uma determinada regra, basta clicar com o botão direito do mouse sobre ela. Aparecerá o seguinte menu: (este menu será acionado sempre que se pressionar o botão direito, mesmo que não exista nenhuma regra selecionada. Neste caso, somente as opções *Incluir* e *Colar* estarão habilitadas)

- **Inserir:** Esta opção permite se incluir uma nova regra na lista. Se alguma regra estiver selecionada, a nova será inserida na posição da regra selecionada. Caso contrário, a nova regra será incluída no final da lista.
- **Editar:** Esta opção abre a janela de edição para a regra selecionada.
- **Apagar**: Esta opção remove da lista a regra selecionada.
- **Copiar:** Esta opção copia a regra selecionada para uma área temporária.
- **Colar:** Esta opção copia a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.
- **Renomear:** Esta opção renomeia a regra selecionada da lista

Dica: Todas as opções mostradas acima podem ser executadas a partir da barra de ferramentas localizada logo acima da lista. Neste caso, primeiro seleciona-se a regra, clicando-o com o botão esquerdo, e em seguida clica-se na opção desejada.

No caso de inclusão ou edição de regras, será mostrada a janela de edição, mostrada abaixo:

A janela de edição de regras DNS reverso



Para se criar uma regra, é necessário se preencher os seguintes campos:

Nome: Nome que define unicamente a regra dentro do contexto. Este nome será mostrado na lista de regras do contexto SMTP. Não podem existir duas regras com o mesmo nome.

Operador de pesquisa: Os mesmos operadores utilizados nas regras de filtragem SMTP podem ser utilizados para a filtragem do DNS reverso.

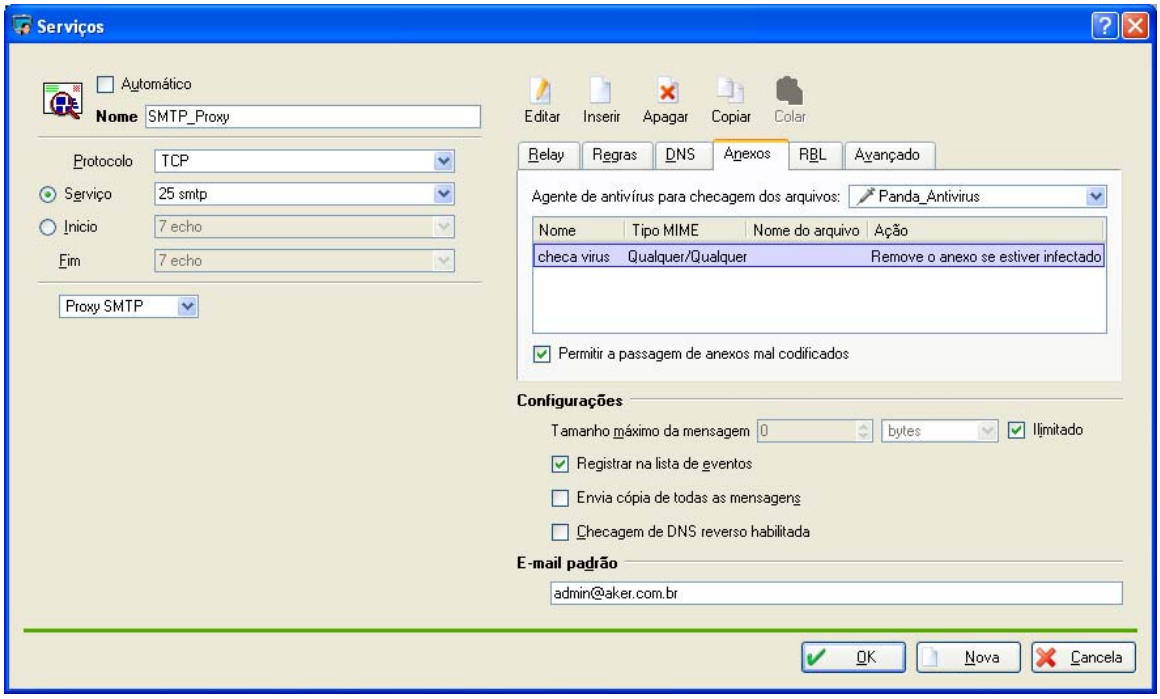
Texto: Define o texto a ser pesquisado.

Registrar na lista de eventos: Registra no log de eventos do firewall caso a regra tenha sido executada.

Verifica alias: Se esta opção estiver marcada, o firewall comparará todos os nomes retornados pelo DNS para verificar se algum deles se encaixa na regra.

Ação: Ação a ser executada pelo firewall caso a regra seja atendida. Ela pode ser Aceita ou Rejeita.

- **Pasta de anexos**



Nessa pasta são especificadas as regras de tratamento de arquivos anexados. Essas regras permitem que, caso uma mensagem tenha sido aceita, ela tenha seus arquivos anexados removidos ou checados contra vírus. Elas permitem também que se rejeite uma mensagem por completo, caso ela contenha um arquivo anexo inaceitável (com vírus, por exemplo).

Agente de antivírus para checagem dos arquivos: Esse campo indica o agente antívirus que será utilizado para se checar vírus dos arquivos anexados a mensagens de e-mail. Esse agente deve ter sido previamente cadastrado no firewall. Para maiores informações veja o capítulo intitulado Cadastrando entidades.

Para se executar qualquer operação sobre uma determinada regra, basta clicar com o botão direito do mouse sobre ela. Aparecerá o seguinte menu: (este menu será acionado sempre que se pressionar o botão direito, mesmo que não exista nenhuma regra selecionada. Neste caso, somente as opções *Incluir* e *Colar* estarão habilitadas)

- **Inserir:** Esta opção permite se incluir uma nova regra na lista. Se alguma regra estiver selecionada, a nova será inserida na posição da regra selecionada. Caso contrário, a nova regra será incluída no final da lista.
- **Editar:** Esta opção abre a janela de edição para a regra selecionada.
- **Apagar**: Esta opção remove da lista a regra selecionada.
- **Copiar:** Esta opção copia a regra selecionada para uma área temporária.

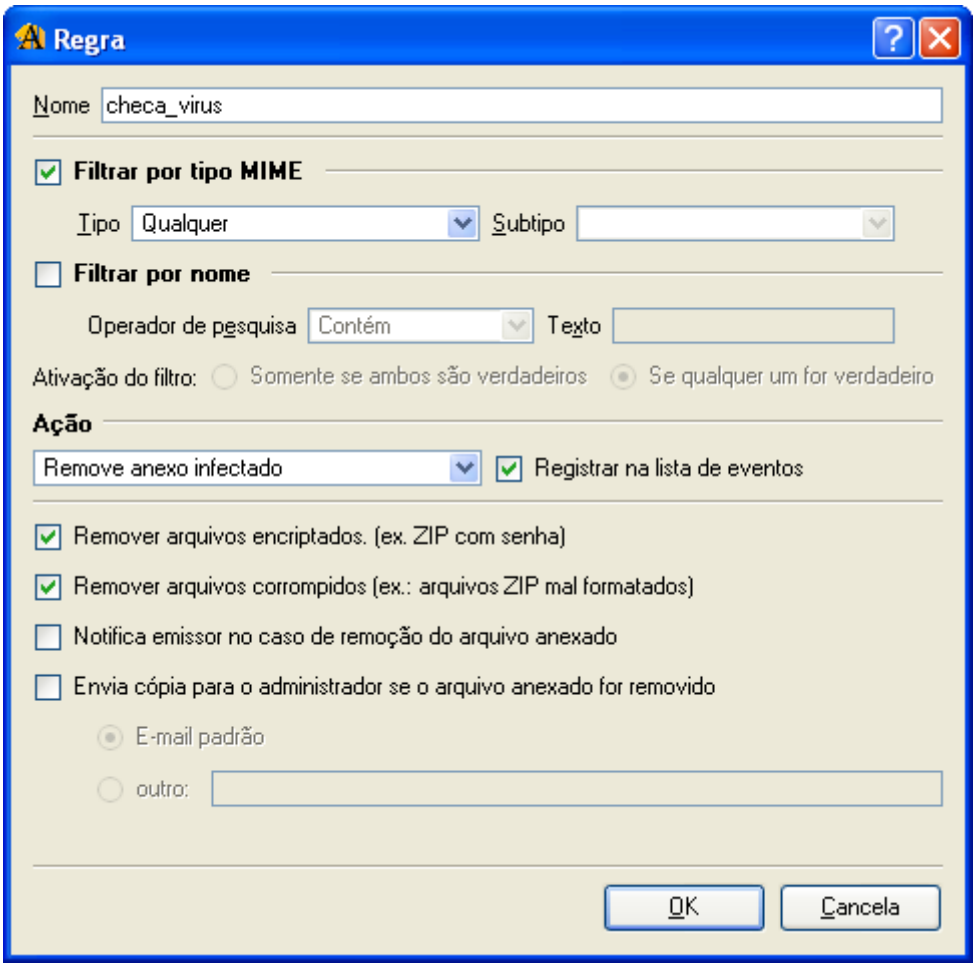
- **Colar:** Esta opção copia a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.
- **Renomear:** Esta opção renomeia a regra selecionada da lista.

Dica: Todas as opções mostradas acima podem ser executadas a partir da barra de ferramentas localizada logo acima da lista. Neste caso, primeiro seleciona-se a regra, clicando-o com o botão esquerdo, e em seguida clica-se na opção desejada.

A ordem das regras na lista de regras de filtragem de arquivos anexados é de fundamental importância. Para cada arquivo anexado de uma mensagem, o firewall pesquisará a lista a partir do início procurando uma regra na qual ele se enquadre. Tão logo uma seja encontrada, a ação associada a ela será executada.

No caso de inclusão ou edição de regras, será mostrada a janela de edição, mostrada abaixo:

A janela de edição de regras de anexos



Nesta janela são configurados todos os parâmetros relativos a uma regra de filtragem de arquivos para um contexto SMTP. Ela consiste dos seguintes campos:

Nome: Nome que define unicamente a regra dentro do contexto. Este nome será mostrado na lista de regras de arquivos. Não podem existir duas regras com o mesmo nome.

Filtrar por tipo MIME: Esse campo permite com que se defina uma regra de filtragem de arquivos baseando-se em seu tipo MIME. Ao ser marcada, deve-se especificar seu tipo e seu subtipo.

Filtrar por nome: Esse campo permite com que se realize filtragems a partir (de parte) do nome, do arquivo anexado. Ao ser marcado, deve-se especificar o tipo de pesquisa a ser efetuada e o texto a ser pesquisado. Estes campos são análogos aos campos de mesmo nome da regra de filtragem SMTP, descrita acima.

Operador de pesquisa: Este campo é análogo ao campo de mesmo nome da regra de filtragem SMTP, descrita acima.

Ação: Indica qual a ação a ser tomada pelo firewall quando um arquivo se enquadrar na regra. Ela consiste de três opções:

- **Aceita o anexo**: Se essa opção for selecionada o firewall irá manter o arquivo anexado na mensagem.
- **Remove o anexo**: Se essa opção for selecionada o firewall irá remover o arquivo anexado da mensagem.
- **Descarta mensagem:** Se essa opção for selecionada o firewall recusará a mensagem completa.
- **Remove anexo infectado**: Se essa opção for selecionada o firewall irá verificar o arquivo anexado da mensagem contra vírus. Caso exista vírus o firewall tomará uma das seguintes ações: se o arquivo puder ser desinfectado, o vírus será removido e o arquivo reanexado à mensagem. Caso o arquivo não possa ser desinfectado, o firewall o removerá e acrescentará uma mensagem informando ao destinatário desse fato.
- **Descarta mensagem infectada**: Se essa opção for selecionada o firewall irá verificar o arquivo anexado da mensagem contra vírus. Caso exista vírus o firewall tomará uma das seguintes ações: se o arquivo puder ser desinfectado, o vírus será removido e o arquivo reanexado à mensagem. Caso o arquivo não possa ser desinfectado, o firewall recusará a mensagem.

Recomenda-se utilizar as ações que removem os arquivos anexados nos emails recebidos pela companhia e as que bloqueiam a mensagem por completo nas regras aplicadas aos emails que saem.

Remove arquivos encriptados: Se essa opção estiver marcada, o firewall removerá os arquivos anexados que estejam cifrados, de forma que não possam ser checados quanto a presença de vírus.

Remove arquivos corrompidos: Se essa opção estiver marcada, o firewall removerá os arquivos anexados que estejam corrompidos.

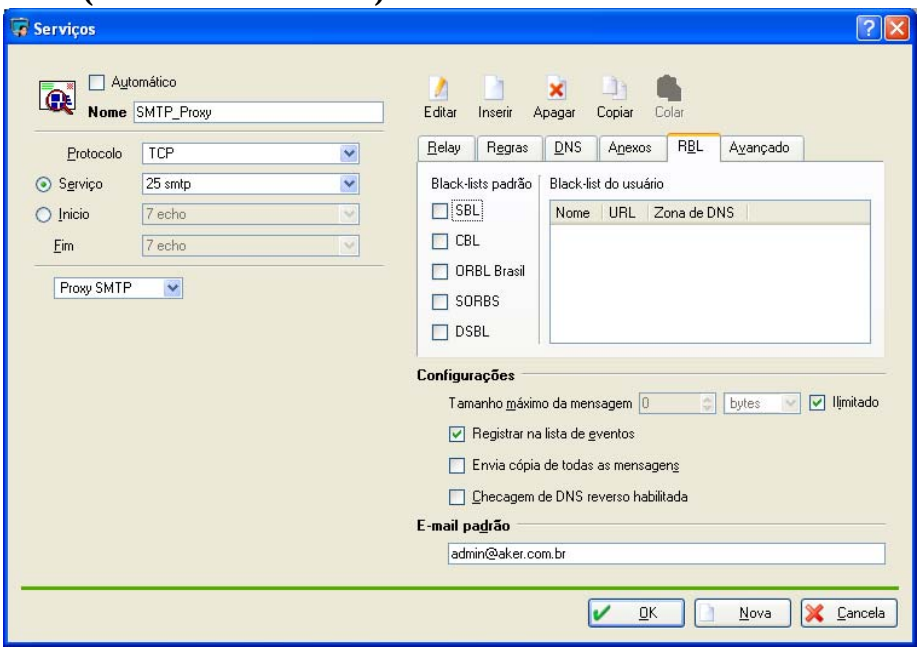
Notifica emissor no caso de remoção do arquivo anexado: Se essa opção estiver marcada, o firewall enviará uma mensagem para o emissor de um e-mail todas as vezes que um ou mais de seus arquivos anexados for removido.

Envia cópia para o administrador do arquivo anexado for removido: Se essa opção estiver marcada, o firewall enviará uma cópia de todos os arquivos removidos para o

administrador. Caso ela esteja marcada, deve-se escolher uma das seguintes opções de envio:

- **Padrão:** A cópia da mensagem é enviada para o e-mail padrão.
- **e-mail:** A cópia da mensagem é enviada para o endereço especificado no campo à direita.

- **Pasta RBL (Real-time Black List)**



Esta pasta contém opções de bloqueio de sites considerados fontes de SPAM. O bloqueio é feito em tempo real, mediante consulta a uma ou mais listas de bloqueio dinâmicas, mantidas por terceiros. Ela consiste das seguintes opções:

Black list padrão: São cinco listas negras que contém vários relays acusados de fazer SPAM (envio de mensagem não desejada). Elas são gerenciadas por organizações e o firewall simplesmente as consulta antes de aceitar os e-mails. Marque as opções correspondentes se desejar utilizar esta facilidade.

- **SBL:** Para saber mais acesse o endereço http://www.spamhaus.com
- **CBL:** Para saber mais acesse o endereço http://cbl.abuseat.org
- **ORBL Brasil:** Para saber mais acesse o endereço http://www.globalmedia.com.br/orbl
- **DSBL:** Para saber mais acesse o endereço http://dsbl.org/

Black list do usuário: São listas negras configuráveis pelo administrador do firewall. Ela consiste de uma lista de listas negras, cada uma com os seguintes campos:

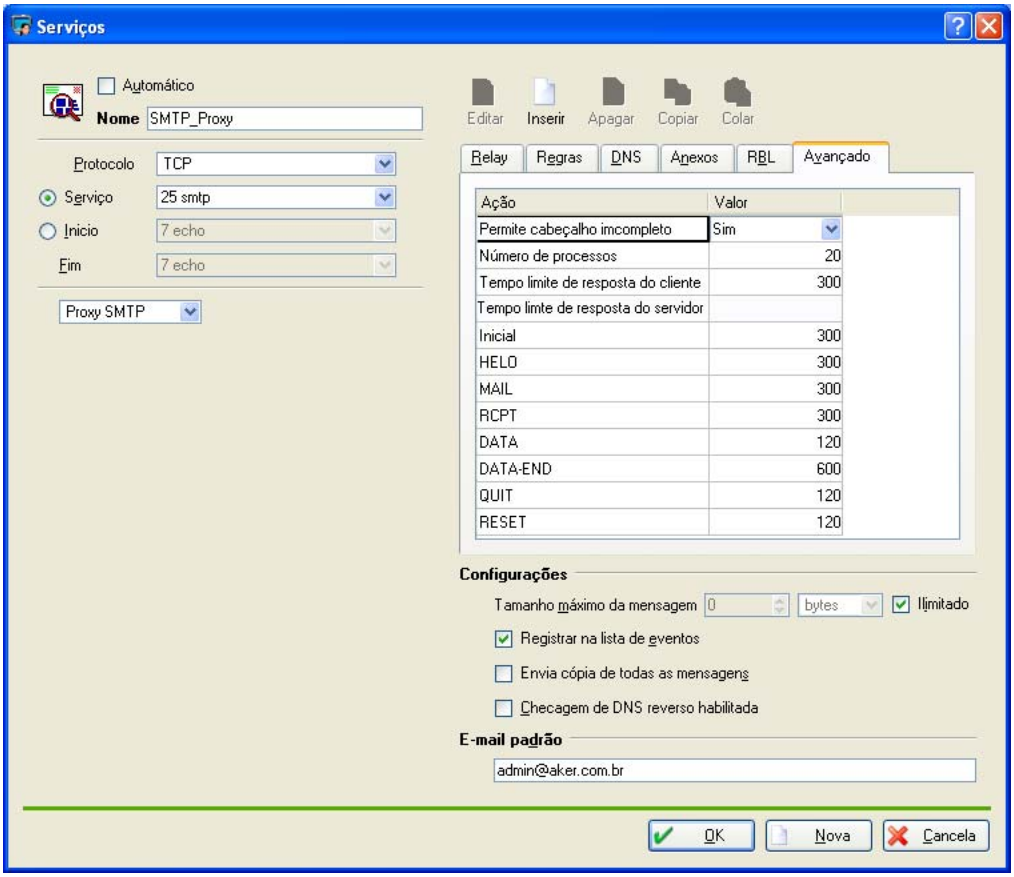
Nome: Nome pelo qual se se deseja chamar a blacklist

URL: URL explicativa para ser mostrada para o usuário que tiver seus e-mails recusados

Zona: É a zona completa de DNS que deverá ser consultada pelo firewall. Caso um endereço IP esteja presente nessa zona, e-mails vindos dele serão recusados.

Alguns serviços de black list costumam ter seu funcionamento interrompido temporariamente devido à problemas de natureza judicial. Quando isto acontece, ou eles se tornam inefetivos ou bloqueiam mais e-mails do que deveriam. Por favor verifique o funcionamento correto da black-list desejada antes de colocá-la em uso.

- **Pasta Avançado**



Esta pasta permite o acesso às opções de configuração avançadas do proxy SMTP. Elas permitem um ajuste fino do funcionamento do proxy. As opções são:

Permite cabeçalho incompleto: Se esta opção estiver marcada como **NÃO**, não serão aceitas mensagens cujos cabeçalhos não contenham todos os campos obrigatórios de uma mensagem SMTP.

Número de processos: Este campo indica o número máximo de cópias do proxy que poderão estar ativas em um determinado momento. Como cada processo trata uma conexão, este número também representa o número máximo de mensagens que podem ser enviadas simultaneamente para o contexto em questão. Caso o número de conexões ativas atinja este limite, os clientes que tentarem enviar novas mensagens serão informados que o servidor se encontra temporariamente impossibilitado de aceitar novas conexões e que devem tentar novamente mais tarde.

É possível se utilizar este número de processos como uma ferramenta para controlar o número máximo de mensagens simultâneas passando pelo link, de forma a não saturá-lo.

Tempo limite de resposta do cliente: Este parâmetro indica o tempo máximo, em segundos, que o proxy espera entre cada comando do cliente que está enviando a mensagem SMTP. Caso este tempo seja atingido, sem receber nenhum comando do cliente, o proxy assume que este caiu e derruba a conexão.

Tempo limite de resposta para servidor: Para cada um dos possíveis comandos válidos do protocolo SMTP, existe um tempo máximo de espera por uma resposta do servidor. Caso não receba nenhuma resposta dentro deste período, o proxy assume que o servidor caiu e derruba a conexão. Neste grupo é possível ser configurar o tempo máximo de espera, em segundos, para cada um destes comandos.

Todos os demais parâmetros se referem aos tempos limites de resposta para cada comando SMTP e não devem ser modificados a não ser que haja uma razão específica para fazê-lo.

23-0 Configurando o proxy Telnet

Neste capítulo será mostrado como se configurar o proxy telnet para realizar autenticação de usuários

O que é o proxy Telnet ?

O proxy Telnet é um programa especializado do Firewall Aker feito para trabalhar com o protocolo Telnet, que é o protocolo utilizado para emulação de terminais remotos. A sua função básica é possibilitar a realização de uma autenticação a nível de usuário para as sessões telnet a serem estabelecidas. Este tipo de autenticação permite uma grande flexibilidade e um elevado nível de segurança.

Ele é um proxy transparente (para maiores informações veja o capítulo intitulado Trabalhando com proxies), desta forma, nem o servidor nem o cliente sabem de sua existência.

Utilizando o proxy Telnet

Para se utilizar o proxy Telnet para realizar autenticações em uma comunicação, é necessário se executar uma seqüência de 2 passos:

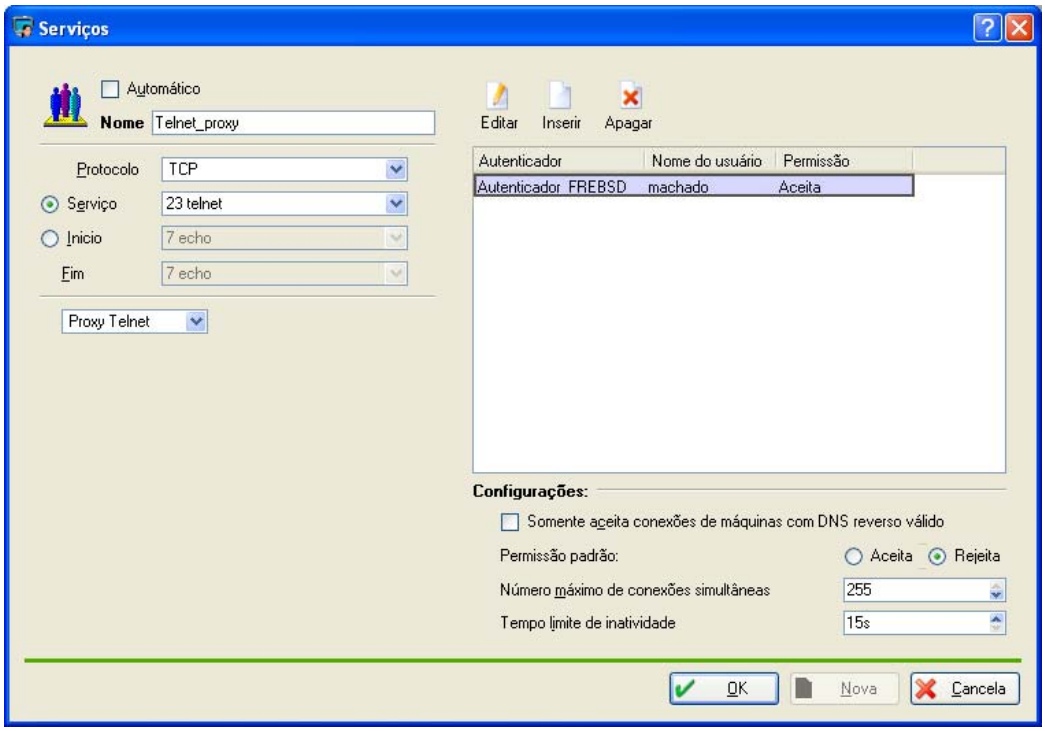
1. Cria-se um serviço que será desviado para o proxy Telnet e edita-se os parâmetros do contexto a ser usado por este serviço (para maiores informações, veja o capítulo intitulado Cadastrando Entidades)
2. Acrescenta-se uma regra de filtragem permitindo o uso do serviço criado no passo 1, para as redes ou máquinas desejadas (para maiores informações, veja o capítulo intitulado Filtro de Estados)

A partir deste momento, todas as vezes que uma sessão telnet que se enquadre na regra criada for estabelecida, o firewall solicitará uma identificação do usuário e uma senha. Se a identificação e a senha forem válidas e o usuário em questão tiver permissão, a sessão será estabelecida. Caso contrário o usuário será informado do erro e a sessão cancelada.

23-1 Editando os parâmetros de um contexto Telnet

A janela de propriedades de um contexto Telnet será mostrada quando a opção **Proxy Telnet** for selecionada. Através dela é possível se definir o comportamento do proxy Telnet quando este for lidar com o serviço em questão.

A janela de propriedades de um contexto Telnet



Na janela de propriedades são configurados todos os parâmetros de um contexto associado a um determinado serviço. Ela consiste dos seguintes campos:

Somente aceita conexões de máquinas com DNS reverso válido: Se esta opção estiver marcada, somente serão aceitas conexões de máquinas cujo DNS reverso esteja configurado e aponte para um nome válido.

Permissão Padrão: Este campo indica a permissão que será aplicada a todos os usuários que não estiverem presentes e que não façam parte de nenhum grupo presente na lista de permissões. O valor *aceita* permite que a sessão de telnet seja estabelecida e o valor *rejeita* impede sua realização.

Número máximo de sessões simultâneas: Este campo define o número máximo de sessões telnet que podem estar ativas simultaneamente neste contexto. Caso o número de sessões abertas atinja este limite, os usuários que tentarem estabelecer novas conexões serão informados que o limite foi atingido e que devem tentar novamente mais tarde.

Tempo limite de inatividade: Este campo define o tempo máximo, em segundos, que o proxy pode ficar sem receber dados da sessão Telnet e ainda considerá-la ativa.

O valor deste campo deve ser menor ou igual ao valor configurado no campo **Tempo limite TCP**, nos parâmetros de configuração globais. (para maiores informações, veja o capítulo intitulado Configurando os parâmetros do sistema)

Lista de permissões: Esta lista define, de forma individual, as permissões de acesso para usuários ou grupos.

Para se executar qualquer operação sobre um usuário ou grupo na lista de permissões, basta clicar com o botão direito do mouse sobre ele. Aparecerá o seguinte menu: (este

menu será acionado sempre que se pressionar o botão direito, mesmo que não exista nenhum usuário/grupo selecionado. Neste caso, somente as opções *Incluir* e *Colar* estarão habilitadas)

- **Inserir:** Esta opção permite se incluir um novo usuário/grupo na lista. Se algum usuário/grupo estiver selecionado, o novo será inserido na posição selecionada. Caso contrário, o novo usuário/grupo será incluído no final da lista.
- **Editar**: Esta opção permite que se altere a permissão de acesso do usuário/grupo selecionado.
- **Apagar**: Esta opção remove da lista o usuário/grupo selecionado.

Dica: Todas as opções mostradas acima podem ser executadas a partir da barra de ferramentas localizada logo acima da lista. Neste caso, primeiro seleciona-se o usuário/grupo, clicando-o com o botão esquerdo, e em seguida clica-se na opção desejada.

A ordem dos usuários e grupos na lista de permissões é de fundamental importância. Quando um usuário se autenticar, o firewall pesquisará a lista a partir do início procurando pelo nome desse usuário ou por um grupo de que ele faça parte. Tão logo um desses seja encontrado, a permissão associada ao mesmo será utilizada.

Para se alterar a posição de um usuário ou grupo dentro da lista, deve-se proceder da seguinte forma:

1. Seleciona-se o usuário ou grupo a ser movido de posição
2. Clica-se em um dos botões em formato de seta, localizados a direita da lista. O botão com o desenho da seta para cima fará com que o usuário/grupo selecionado seja movido uma posição para cima. O botão com a seta para baixo fará com que este seja movido uma posição para baixo.

No caso de inclusão de usuários/grupos, será mostrada a seguinte janela:

A janela de inclusão de usuários/grupos

A janela de inclusão permite definir a permissão de acesso para um usuário ou um grupo de um determinado autenticador. Para fazê-lo, deve-se proceder da seguinte forma:

Seleciona-se o autenticador do qual se deseja obter a lista de usuários ou grupos, clicando-se com o botão esquerdo sobre seu nome na lista superior da janela (se o autenticador desejado não aparecer na lista, é necessário acrescentá-lo na lista de autenticadores a serem pesquisados. Para maiores informações, veja o capítulo intitulado Configurando parâmetros de autenticação).

1. Seleciona-se entre listagem de usuários ou grupos, clicando-se nos botões correspondentes localizados entre as duas listas.
2. Clica-se com o botão esquerdo sobre o nome do usuário ou grupo que se deseja incluir, na lista inferior da janela.
3. Define-se a permissão de acesso para o usuário ou grupo, escolhendo entre os valores *aceita* (que possibilitará o estabelecimento da sessão) ou *rejeita* (que impedirá seu estabelecimento).
4. Clica-se no botão **OK**, o que provocará o fechamento da janela e a inclusão do usuário ou grupo na lista de permissões da janela de propriedades do contexto.

24-0 Configurando o proxy FTP

Neste capítulo será mostrado como se configurar o proxy FTP, de forma a bloquear determinados comandos da transferência de arquivos

O que é o proxy FTP ?

O proxy FTP é um programa especializado do Firewall Aker feito para trabalhar com o protocolo FTP, que é o protocolo utilizado para a transferência de arquivos pela Internet. A sua função básica é possibilitar que o administrador defina que comandos podem ser aceitos e impedir, por exemplo, a criação de novos arquivos ou de diretórios.

Ele é um proxy transparente (para maiores informações veja o capítulo intitulado Trabalhando com proxies), desta forma, nem o servidor nem o cliente sabem de sua existência.

Utilizando o proxy FTP

Para se utilizar o proxy FTP para realizar o controle de uma transferência de arquivos, é necessário se executar uma seqüência de 2 passos:

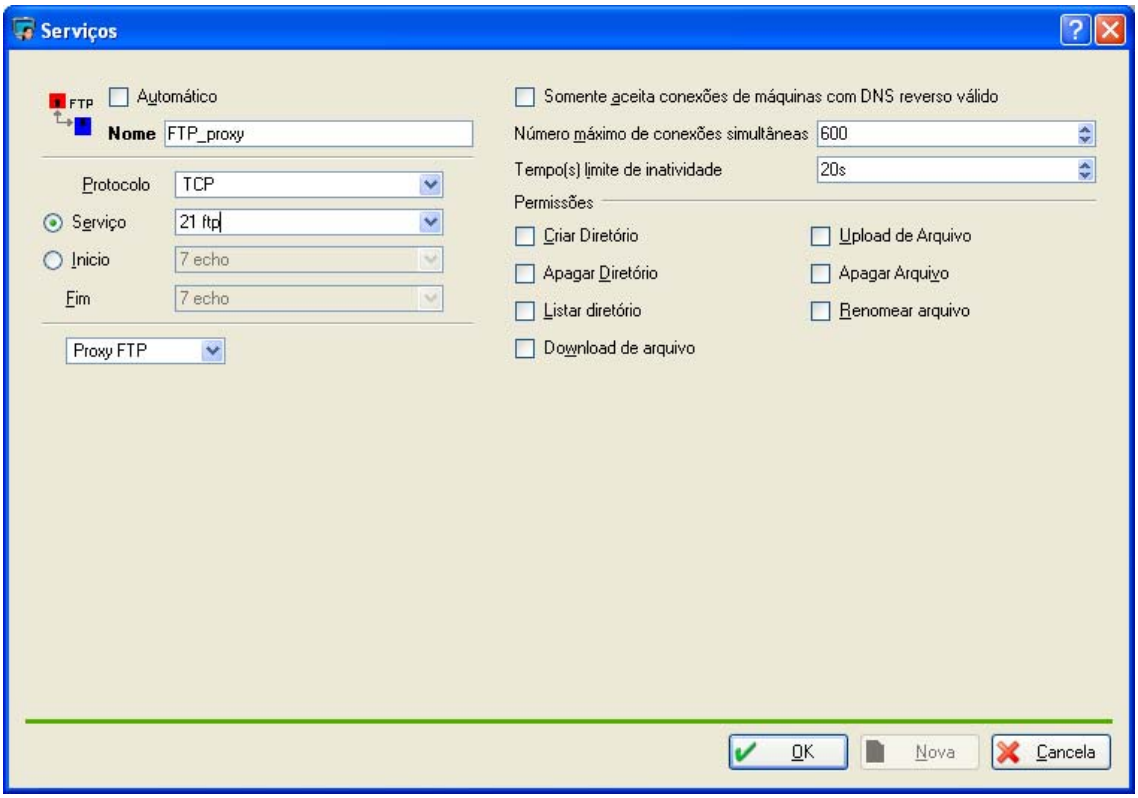
1. Cria-se um serviço que será desviado para o proxy FTP e edita-se os parâmetros do contexto a ser usado por este serviço (para maiores informações, veja o capítulo intitulado Cadastrando Entidades)
2. Acrescenta-se uma regra de filtragem permitindo o uso do serviço criado no passo 1, para as redes ou máquinas desejadas (para maiores informações, veja o capítulo intitulado Filtro de Estados)

O proxy FTP não realiza autenticação de usuários. Para possibilitar que certos usuários tenham privilégios diferentes, é necessário criar serviços do proxy FTP com contextos distintos e associar cada um destes serviços com um perfil de acesso. Para maiores informações sobre perfis de acesso, verifique o capítulo chamado Perfis de acesso de usuários.

24-1 Editando os parâmetros de um contexto FTP

A janela de propriedades de um contexto FTP será mostrada quando se selecionar a opção **Proxy FTP**, na janela de edição de serviços. Através dela é possível se definir o comportamento do proxy FTP quando este for lidar com o serviço em questão.

A janela de propriedades de um contexto FTP



Na janela de propriedades são configurados todos os parâmetros de um contexto associado a um determinado serviço. Ela consiste dos seguintes campos:

Somente aceita conexões de máquinas com DNS reverso válido: Se esta opção estiver marcada, somente serão aceitas conexões de máquinas cujo DNS reverso esteja configurado e aponte para um nome válido.

Número máximo de conexões simultâneas: Este campo define o número máximo de sessões FTP que podem estar ativas simultaneamente neste contexto. Caso o número de sessões abertas atinja este limite, os usuários que tentarem estabelecer novas conexões serão informados que o limite foi atingido e que devem tentar novamente mais tarde.

Tempo limite de inatividade: Este campo define o tempo máximo, em segundos, que o proxy pode ficar sem receber dados da sessão FTP e ainda considerá-la ativa.

O valor deste campo deve ser menor ou igual ao valor configurado no campo **Tempo limite TCP**, nos parâmetros de configuração globais. (para maiores informações, veja o capítulo intitulado Configurando os parâmetros do sistema)

Criar diretório: Se esta opção estiver desmarcada, não será possível a criação de diretórios através das conexões FTP que se encaixarem neste contexto.

Apagar diretório: Se esta opção estiver desmarcada, não será possível a remoção de diretórios através das conexões FTP que se encaixarem neste contexto.

Listar diretório: Se esta opção estiver desmarcada, não será possível a visualização do conteúdo de diretórios (comandos `DIR` ou `LS`) através das conexões FTP que se encaixarem neste contexto.

Download de arquivos: Se esta opção estiver desmarcada, não será possível se fazer download de arquivos através das conexões FTP que se encaixarem neste contexto.

Upload de arquivos: Se esta opção estiver desmarcada, não será possível se fazer upload de arquivos através das conexões FTP que se encaixarem neste contexto.

Apagar arquivos: Se esta opção estiver desmarcada, não será possível se remover arquivos através das conexões FTP que se encaixarem neste contexto.

Renomear arquivos: Se esta opção estiver desmarcada, não será possível se renomear arquivos através das conexões FTP que se encaixarem neste contexto.

25-0 Configurando o proxy POP3

Neste capítulo serão mostradas quais as funções oferecidas pelo proxy POP3 e como realizar sua configuração

O que é o proxy POP3 ?

O proxy POP3 é um programa especializado do Firewall Aker feito para trabalhar com correio eletrônico (POP3 é um anagrama para *Post Office Protocol*, que é o nome completo do serviço de download de mensagens de correio eletrônico na Internet). Este proxy possibilita que sejam realizadas filtragens de e-mails baseadas em seus arquivos anexos. Ele também atua como uma barreira protegendo o servidor POP3 contra diversos tipos de ataques.

Ele é um proxy transparente (para maiores informações veja o capítulo intitulado Trabalhando com proxies), desta forma, nem o servidor nem o cliente sabem de sua existência.

Ataques contra um servidor POP3

Existem diversos ataques passíveis de serem realizados contra um servidor POP3. São eles:

- **Ataques explorando *bugs* de um servidor**

Neste caso, o atacante procura utilizar um comando ou parâmetros de um comando que conhecidamente provocam falhas de segurança.
O proxy POP3 do Firewall Aker impede estes ataques na medida em que só permite a utilização de comandos considerados seguros e validando os parâmetros de todos os comandos.

- **Ataques explorando estouro de áreas de memória (*buffer overflows*)**

Estes ataques consistem em se enviar linhas de comando muito grandes, fazendo com que um servidor que não tenha sido corretamente desenvolvido apresente falhas de segurança.

O proxy POP3 do Firewall Aker impede estes ataques na medida em que limita o tamanho máximo das linhas de comando que podem ser enviadas para o servidor.

Utilizando o proxy POP3

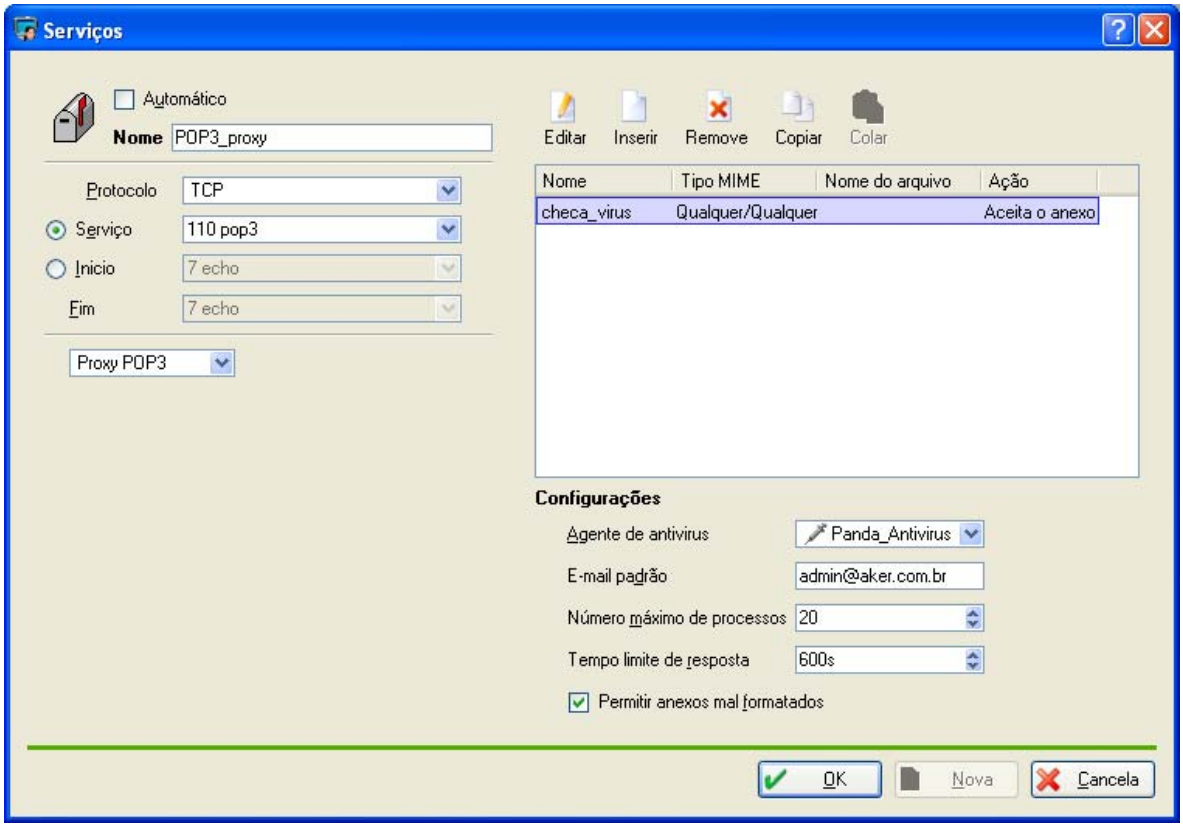
Para se utilizar o proxy POP3 em uma comunicação, é necessário se executar uma seqüência de 2 passos:

1. Cria-se um serviço que será desviado para o proxy POP3 e edita-se os parâmetros do contexto a ser usado por este serviço (para maiores informações, veja o capítulo intitulado Cadastrando Entidades)
2. Acrescenta-se uma regra de filtragem permitindo o uso do serviço criado no passo 1, para as redes ou máquinas desejadas (para maiores informações, veja o capítulo intitulado Filtro de Estados)

25-1 Editando os parâmetros de um contexto POP3

A janela de propriedades de um contexto POP3 será mostrada quando a opção **Proxy POP3** for selecionada. Através dela é possível se definir o comportamento do proxy POP3 quando este for lidar com o serviço em questão.

A janela de propriedades de um contexto POP3



Na janela de propriedades são configurados todos os parâmetros de um contexto associado a um determinado serviço. São eles:

Configurações: É formado por diversos campos que indicam as ações a serem executadas pelo proxy POP3:

- **Agente antivírus**: Esse campo indica o agente anti-virus que será utilizado para se checar vírus dos arquivos anexados a mensagens de e-mail. Esse agente deve ter sido previamente cadastrado no firewall. Para maiores informações veja o capítulo intitulado Cadastrando entidades.
- **E-mail padrão:** Indica o endereço de e-mail padrão, para o qual serão enviadas as cópias das mensagens que não se enquadrarem em nenhuma regra deste

contexto (se a opção Envia Cópia estiver marcada). Este e-mail também pode ser referenciado em qualquer regra de filtragem do contexto.

- **Número máximo de processos:** Este campo indica o número máximo de cópias do proxy que poderão estar ativas em um determinado momento. Como cada processo trata uma conexão, este número também representa o número máximo de mensagens que podem ser transmitidas simultaneamente para o contexto em questão. Caso o número de conexões ativas atinja este limite, os clientes que tentarem enviar novas mensagens deverão repetir a tentativa posteriormente.
- **Tempo limite de resposta:** Este parâmetro indica o tempo máximo, em segundos, que o proxy espera a conexão em inatividade. Caso este tempo seja atingido o proxy encerra a conexão.
- **Permitir a passagem de anexos mal codificados:** Permite que anexos que estejam mal codificados passem pelo firewall e sejam entregues aos clientes de email.

Lista de regras: Nessa lista são especificadas as regras de tratamento de arquivos anexados que permitem que uma mensagem tenha seus arquivos anexados removidos ou checados contra vírus.

Para se executar qualquer operação sobre uma determinada regra, basta clicar com o botão direito do mouse sobre ela. Aparecerá o seguinte menu: (este menu será acionado sempre que se pressionar o botão direito, mesmo que não exista nenhuma regra selecionada. Neste caso, somente as opções *Incluir* e *Colar* estarão habilitadas)

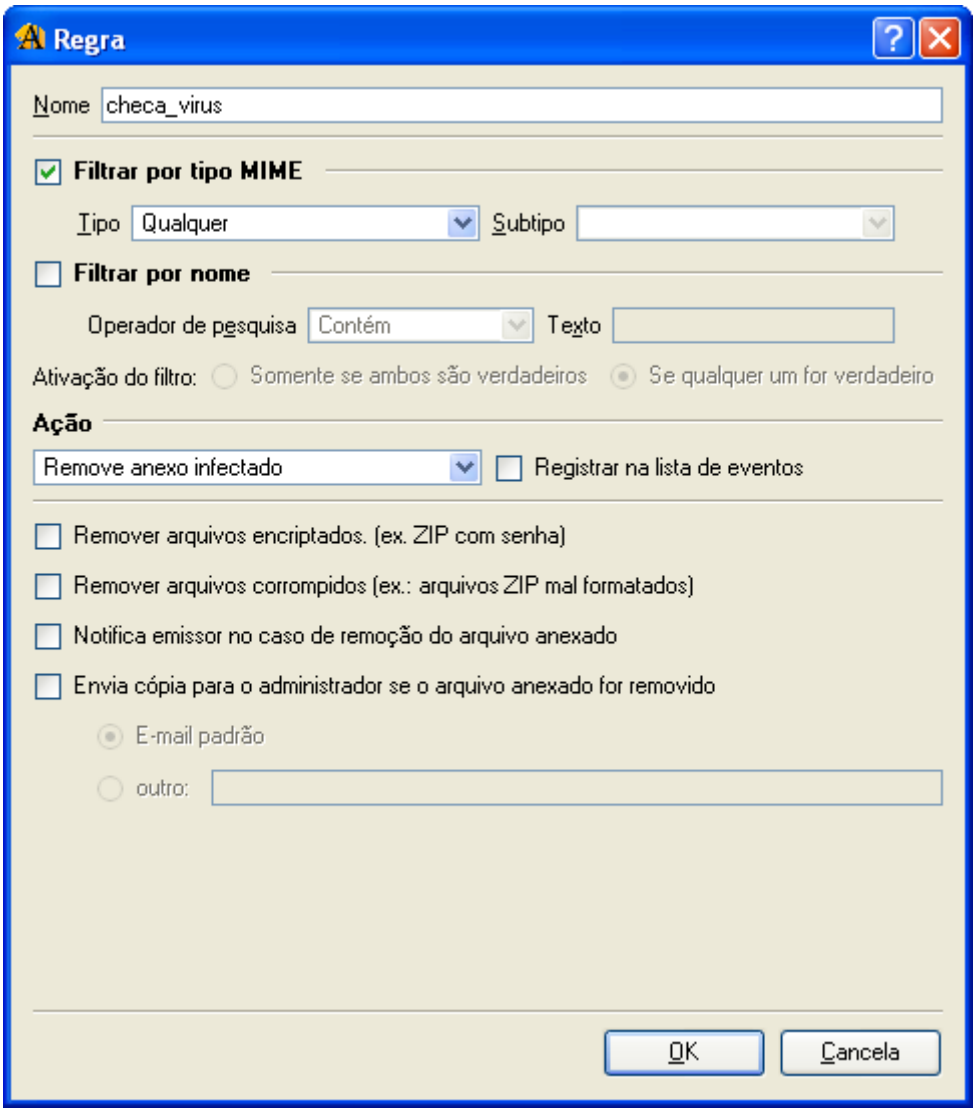
- **Inserir:** Esta opção permite se incluir uma nova regra na lista. Se alguma regra estiver selecionada, a nova será inserida na posição da regra selecionada. Caso contrário, a nova regra será incluída no final da lista.
- **Editar:** Esta opção abre a janela de edição para a regra selecionada.
- **Apagar**: Esta opção remove da lista a regra selecionada.
- **Copiar:** Esta opção copia a regra selecionada para uma área temporária.
- **Colar:** Esta opção copia a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.
- **Renomear:** Esta opção renomeia a regra selecionada.

Dica: Todas as opções mostradas acima podem ser executadas a partir da barra de ferramentas localizada logo acima da lista. Neste caso, primeiro seleciona-se a regra, clicando-o com o botão esquerdo, e em seguida clica-se na opção desejada.

A ordem das regras na lista de regras de filtragem de arquivos anexados é de fundamental importância. Para cada arquivo anexado de uma mensagem, o firewall

pesquisará a lista a partir do início procurando uma regra na qual ele se enquadre. Tão logo uma seja encontrada, a ação associada a ela será executada.
No caso de inclusão ou edição de regras, será mostrada a janela de edição, mostrada abaixo:

A janela de edição de regras de arquivos



Nesta janela são configurados todos os parâmetros relativos a uma regra de filtragem de arquivos para um contexto POP3. Ela consiste dos seguintes campos:
Nome: Nome que define unicamente a regra dentro do contexto. Este nome será mostrado na lista de regras de arquivos. Não podem existir duas regras com o mesmo nome.

Filtrar por tipo MIME: Esse campo permite com que se defina uma regra de filtragem de arquivos baseando-se em seu tipo MIME. Ao ser marcada, deve-se especificar seu tipo e seu subtipo.

Filtrar por nome: Esse campo permite com que se realize filtragems a partir (de parte) do nome, do arquivo anexado. Ao ser marcado, deve-se especificar o tipo de pesquisa a

ser efetuada e o texto a ser pesquisado. As seguintes opções de pesquisa estão disponíveis:

- **CONTÉM:** O nome deve conter o texto informado em qualquer posição.
- **NÃO CONTÉM:** O nome não pode conter o texto informado.
- **É:** O conteúdo do nome deve ser exatamente igual ao texto informado.
- **NÃO É:** O conteúdo do nome deve ser diferente do texto informado.
- **COMEÇA COM:** O conteúdo do nome deve começar com o texto informado.
- **NÃO COMEÇA COM:** O conteúdo do nome não pode começar com o texto informado.
- **TERMINA COM:** O conteúdo do nome deve terminar com o texto informado
- **NÃO TERMINA COM:** O conteúdo do nome não pode terminar com o texto informado.
- **CONTÉM PALAVRAS:** Neste tipo de pesquisa, o texto informado é considerado como formado por palavras individuais (separadas por espaços), ao invés de um texto contínuo. Para se enquadrar na pesquisa, o nome deve conter todas as palavras informadas, independente de sua posição.

Ativação do filtro: Caso se tenha especificado filtragem por tipo MIME e por nome, esse campo permite especificar se a regra deve ser aplicada **Somente se ambos são verdadeiros** (valor **E**) ou **Se qualquer um for verdadeiro** (valor **OU**).

Ação: Indica qual a ação a ser tomada pelo firewall quando um arquivo se enquadrar na regra. Ela consiste de três opções:

- **Aceita o anexo**: Se essa opção for selecionada o firewall irá manter o arquivo anexado na mensagem.
- **Remove o anexo**: Se essa opção for selecionada o firewall irá remover o arquivo anexado da mensagem.
- **Remove anexo infectado**: Se essa opção for selecionada o firewall irá verificar o arquivo anexado da mensagem contra vírus. Caso exista vírus o firewall tomará uma das seguintes ações: se o arquivo puder ser desinfectado, o vírus será removido e o arquivo reanexado à mensagem. Caso o arquivo não possa ser desinfectado, o firewall o removerá e acrescentará uma mensagem informando o destinatário desse fato.

Caso a caixa **Registrar na lista de eventos** estiver marcada, quando a regra for atendida a mesma será registrada no log de eventos.

Remover arquivos encriptados: Se essa opção estiver marcada, o firewall removerá os arquivos anexados que estejam compactados e cifrados, porque não poderá examiná-los para testar a presença de vírus.

Remover arquivos corrompidos: Se essa opção estiver marcada, o firewall removerá os arquivos anexados que estejam compactados porém corrompidos, porque não poderá examiná-los para testar a presença de vírus.

Notifica emissor no caso de remoção do arquivo anexado: Se essa opção estiver marcada, o firewall enviará uma mensagem para o emissor de um e-mail todas as vezes que um ou mais de seus arquivos anexados for removido.

Envia cópia para o administrador se o arquivo anexado for removido: Se essa opção estiver marcada, o firewall enviará uma cópia de todos os arquivos removidos para o administrador. Caso ela esteja marcada, deve-se escolher uma das seguintes opções de envio:

- **E-mail Padrão:** A cópia da mensagem é enviada para o e-mail padrão, definido na janela de propriedades do contexto
- **outro:** A cópia da mensagem é enviada para o endereço especificado no campo à direita.

26-0 Configurando o proxy WWW

Neste capítulo mostraremos para que serve e como configurar o proxy WWW

26-1 Planejando a instalação

O que é o proxy WWW do Firewall Aker?

O proxy WWW é um programa especializado do Firewall Aker feito para trabalhar com os protocolos que compõem a chamada WWW (*World Wide Web*). Dentre entre estes protocolos, estão o HTTP, HTTPS, FTP e Gopher.

Este proxy WWW possui como principal função controlar o acesso dos usuários internos à Internet, definindo quais usuários podem acessar quais páginas, ou quais podem ou não transferir arquivos, por exemplo. Além disso, ele pode bloquear tecnologias consideradas perigosas para algumas instalações como o Active-X™, scripts (JavaScript) e até applets Java™. Mais ainda, ele possibilita a remoção dos banners das páginas, de forma a aumentar a sua velocidade de carga e reduzir a utilização do link.

Ele é um proxy simultaneamente transparente (apenas para HTTP) e não transparente (para maiores informações, veja o capítulo intitulado Trabalhando com proxies), facilitando a instalaçã do sistema.

Quando utilizado da forma transparente, o proxy é normalmente mais rápido do que quando utilizado como um proxy normal, além de não necessitar configuração extra nos clientes. Por outro lado, a capacidade de filtrar URLs para os protocolos HTTPS, FTP e GOPHER só existe no proxy normal.

Para que o proxy não transparente tenha a mesma performance do transparente, é necessário que os browsers suportem o envio de requisições HTTP 1.1 via proxies.

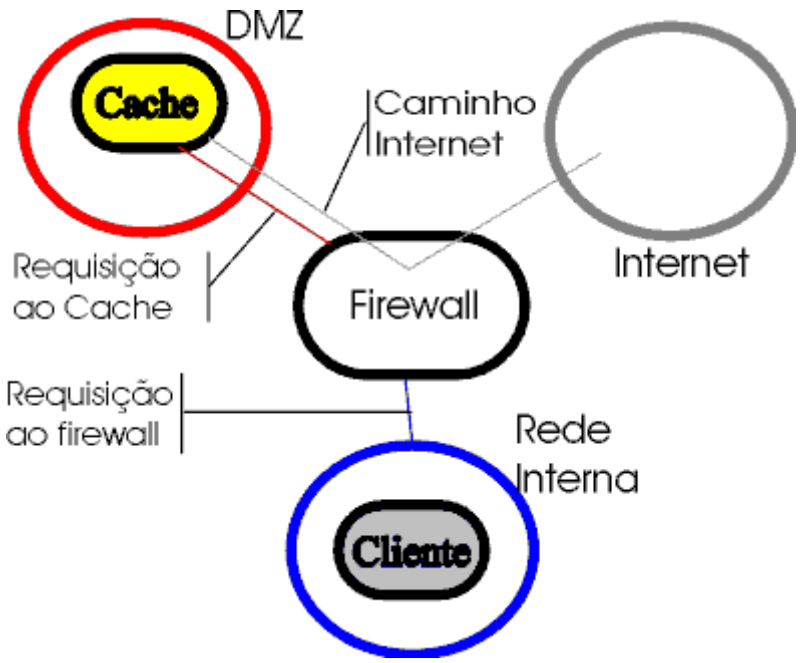
O que é um servidor de cache WWW ?

Um servidor de cache é um programa que visa aumentar o velocidade de acesso às páginas da Internet. Para conseguir isso, ele armazena internamente as páginas mais utilizadas pelas diversas máquinas clientes e todas as vezes que recebe uma nova solicitação, ele verifica se a página desejada já se encontra armazenada. Caso a página esteja disponível, ela é retornada imediatamente, sem a necessidade de se consultar o servidor externo, caso contrário a página é carregada normalmente do servidor desejado e armazenada, fazendo com que as próximas requisições a esta página sejam atendidas rapidamente.

O proxy WWW do Firewall Aker trabalhando com um servidor de cache

O Firewall Aker não implementa por si só um servidor de cache no seu proxy WWW, entretanto ele pode ser configurado para trabalhar com qualquer um que siga os padrões de mercado. Este servidor de cache pode estar rodando na própria máquina onde o firewall se encontra ou em uma máquina separada.

Caso se utilize um servidor de cache em uma máquina separada (modo de instalação recomendado), esta máquina deve ficar em uma sub-rede diferente de onde estão as máquinas clientes, caso contrário todo o controle de segurança pode ser facilmente ultrapassado. Este tipo de configuração pode ser visualizado na seguinte figura:



Neste tipo de instalação, para se assegurar uma total proteção, basta se configurar o filtro de estados (para maiores informações, veja o capítulo intitulado O Filtro de Estados) de forma a permitir que a máquina com o cache seja a única que possa acessar os serviços ligados ao WWW, e que as máquinas clientes não possam abrir nenhuma conexão em direção à máquina onde se encontra o cache. Feito isso, configura-se todas as máquinas clientes para utilizarem o proxy WWW do firewall e configura-se o firewall para utilizar o cache na máquina desejada.

Utilizando o proxy WWW

Para se utilizar o proxy WWW do Firewall Aker no modo não transparente (normal) , é necessária a seguinte seqüência de passos:

1. Cria-se os perfis de acesso desejados e os associa-se com os usuários e grupos desejados. Isso foi descrito no capítulo chamado Perfis de acesso de usuários)
2. Edita-se os parâmetros de configuração do proxy WWW (isso será mostrado no tópico chamado Editando os parâmetros do proxy WWW).

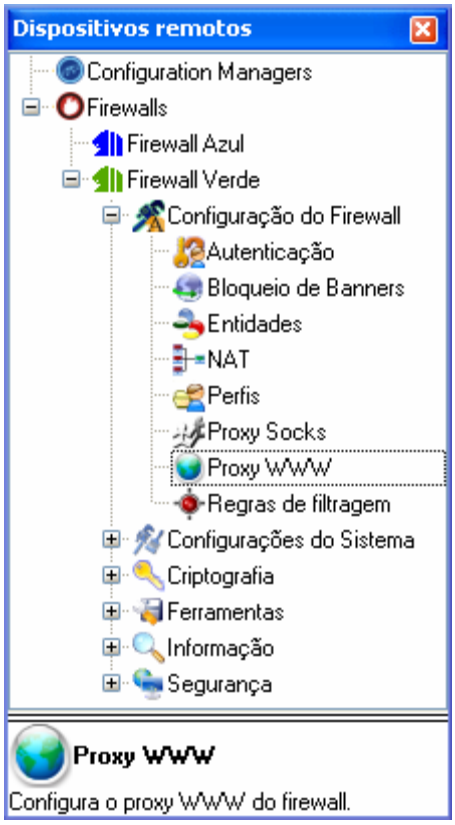
3. Cria-se uma regra de filtragem possibilitando que as máquinas clientes tenham acesso ao proxy (para maiores informações, veja o capítulo intitulado O Filtro de Estados).

O proxy WWW não transparente escuta conexões na porta 80, utilizando o protocolo TCP. Caso seja necessário, pode-se alterar este valor para qualquer porta, bastando para isso acrescentar o parâmetro **-p *porta***, onde *porta* é o número da porta que se deseje que ele escute, na hora de se iniciá-lo. Esta chamada se encontra no arquivo **/etc/firewall/rc.aker**, e deve ser alterada de **/etc/firewall/fwhttppd** para **/etc/firewall/fwhttppd -p 8080**, por exemplo. Para se utilizar o proxy WWW no modo transparente (apenas protocolo HTTP) é necessário se executar uma seqüência de 2 passos:

1. Cria-se um serviço que será desviado para o proxy WWW transparente (HTTP) e edita-se os parâmetros do contexto a ser usado por este serviço (para maiores informações, veja o capítulo intitulado Cadastrando Entidades)
2. Acrescenta-se uma regra de filtragem permitindo o uso do serviço criado no passo 1, para as redes ou máquinas desejadas (para maiores informações, veja o capítulo intitulado Filtro de Estados)

26-2 Editando os parâmetros do Proxy WWW

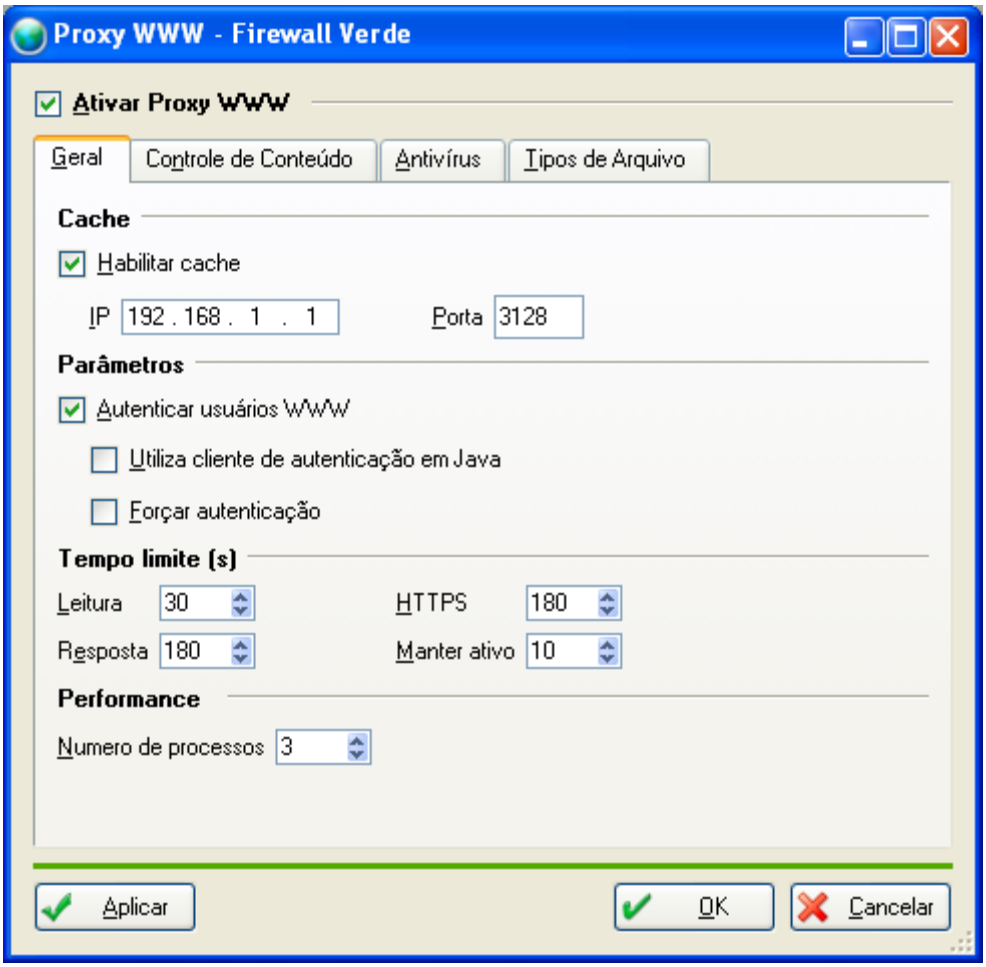
Para se utilizar o proxy WWW, é necessário a definição de alguns parâmetros que determinarão características básicas de seu funcionamento. Esta definição é feita na janela de configuração do proxy WWW. Para acessá-la, basta:



- Clicar no menu *Configuração do Firewall* da janela do firewall

- Selecionar o item *Proxy WWW*

A janela de configuração de parâmetros do proxy WWW



- O botão **OK** fará com que a janela de configuração do proxy WWW seja fechada e as alterações salvas
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta
- O botão **Cancelar**, fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.

Pasta geral

- **Cache**

Habilitar cache: Esta opção permite definir se o proxy WWW irá redirecionar suas requisições para um servidor de cache. Caso esta opção esteja habilitada, todas as requisições recebidas serão repassadas para o servidor de cache, no endereço IP e porta especificados. Caso contrário, o proxy WWW atenderá todas as requisições.

IP: Este campo especifica o endereço IP do servidor de cache para onde as requisições serão redirecionadas, caso a opção *habilita cache* estiver ativa.
Porta: Este campo especifica a porta na qual o servidor de cache espera receber conexões, caso a opção *habilita cache* estiver ativa.

- **Parâmetros**

Esta pasta possibilita ajustar o funcionamento do proxy WWW para situações especiais. Ela consiste dos seguintes campos:
Autentica usuários WWW: Este campo ativa ou não a autenticação de usuários do proxy WWW. Caso ele esteja marcado, será solicitada ao usuário uma identificação e uma senha todas as vezes que ele tentar iniciar uma sessão e esta somente será iniciada caso ele seja autenticado por algum dos autenticadores.
Utiliza cliente de autenticação em Java: Esta opção instrui o proxy a utilizar o cliente de autenticação em Java, mesmo quando operando de modo não transparente. A vantagem deste cliente é permitir que a autenticação do usuário seja completa (como quando se usa o cliente de autenticação para Windows, e não apenas para o proxy WWW).
Caso o usuário esteja utilizando o Cliente de Autenticação Aker para Windows e esteja com uma sessão estabelecida com o Firewall, então não será solicitado nome nem senha, ou seja, o proxy se comportará como se não estivesse realizando autenticação de usuários, mas ele está de fato fazendo-o. Se a sessão do Cliente de Autenticação for finalizada, então o proxy solicitará um nome de usuário e senha no próximo acesso. Para maiores informações sobre o Cliente de Autenticação Aker, leia o capítulo O cliente de autenticação Aker).
Para o cliente de autenticação em Java funcionar em seu browser, ele deve ter o suporte a Java instalado e habilitado, além de permitir o uso do protocolo UDP para applets Java. Apenas o Internet Explorer da Microsoft traz esta opção desabilitada por padrão, e, para habilitá-la você deve escolher configurações personalizadas de segurança para Java e liberar o acesso a todos os endereços de rede para applets não assinados.
Forçar autenticação: Se esta opção estiver marcada o proxy obrigará a autenticação do usuário, ou seja, somente permitirá acesso para usuários autenticados. Se ela estiver desmarcada e um usuário desejar se autenticar, ele poderá fazê-lo (para ganhar um perfil diferente do padrão), mas acessos não identificados serão permitidos.

- **Tempos Limites**

leitura: Este parâmetro define o tempo máximo, em segundos, que o proxy aguarda por uma requisição do cliente, a partir do momento que uma nova conexão for estabelecida. Caso este tempo seja atingido sem que o cliente faça uma requisição, a conexão será cancelada.

resposta: Este parâmetro define o tempo máximo, em segundos, que o proxy aguarda por uma resposta de uma requisição enviada para o servidor WWW remoto ou para o servidor de cache, caso a opção *habilita cache* esteja ativa. Caso este tempo seja atingido sem que o servidor comece a transmitir uma resposta, a conexão com o servidor será cancelada e o cliente receberá uma mensagem de erro.

HTTPS: Este parâmetro define o tempo máximo, em segundos, que o proxy pode ficar sem receber dados do cliente ou do servidor em uma conexão HTTPS, sem que ele considere a conexão inativa e a cancele.

keep-alive: Este parâmetro define quanto tempo um usuário pode manter uma conexão keep-alive (HTTP 1.1) com o proxy inativa, antes que o proxy a encerre, liberando o processo para outro usuário. Recomenda-se manter este tempo bastante baixo, para evitar o uso desnecessário de todos os processos do sistema.

- **Performance**

Número de processos: Este campo define o número de processos do proxy WWW que vão permanecer ativos aguardando conexões. Como cada processo atende uma única conexão, este campo também define o número máximo de requisições que podem ser atendidas simultaneamente.

Por razões de performance, os processos do proxy WWW ficarão ativos sempre, independente de estarem ou não atendendo requisições. Isto é feito com o objetivo de aumentar a performance.

Normalmente, deve-se trabalhar com valores entre 5 e 60 neste campo, dependendo do número de máquinas clientes que utilizarão o proxy (cabe ressaltar que uma única máquina costuma abrir até 4 conexões simultâneas ao acessar uma única página WWW). O valor 0 inviabiliza a utilização do proxy.

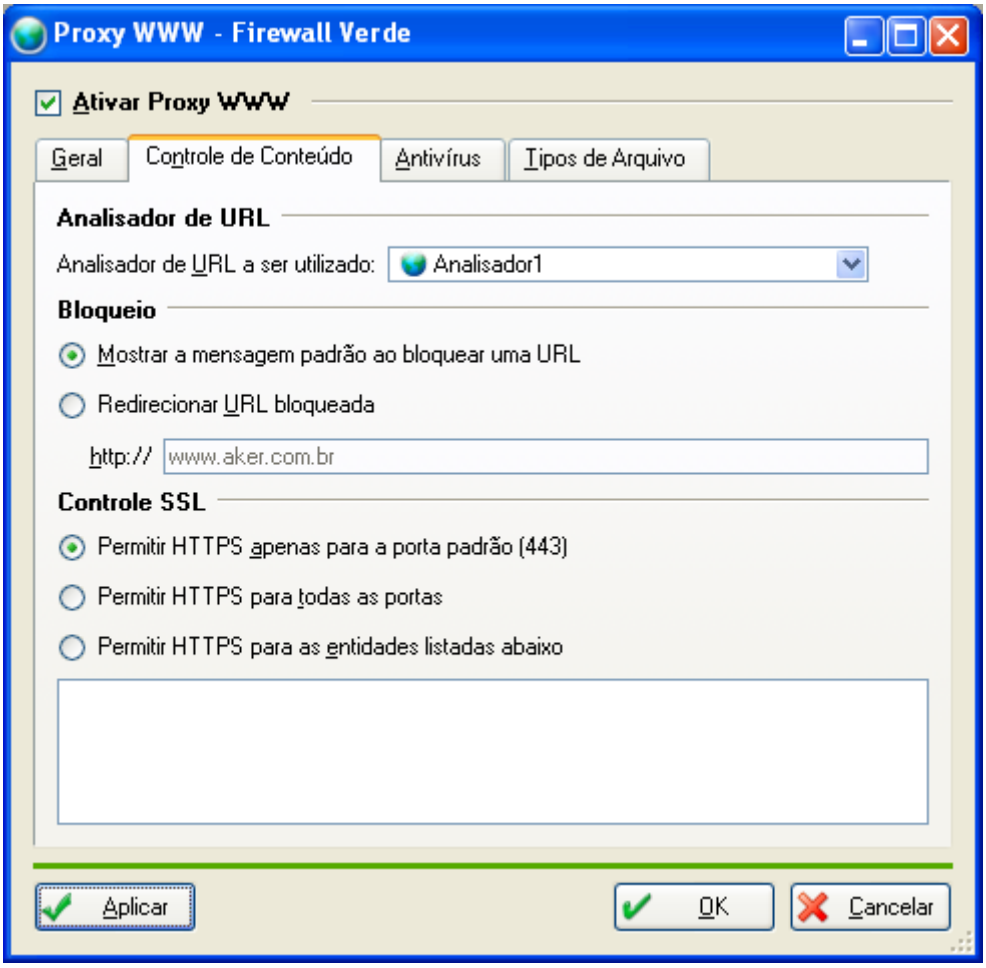
- **Bloqueio**

Essa opção permite se configurar qual ação deve ser executada pelo firewall quando um usuário tentar acessar uma URL não permitida. Ela consiste das seguintes opções:

Mostra mensagem padrão ao bloquear URL: Se essa opção estiver selecionada, o firewall mostrará uma mensagem de erro informando que a URL que se tentou acessar se encontra bloqueada.

Redireciona URL bloqueada: Se essa opção estiver selecionada, o firewall redirecionará todas as tentativas de acesso a URLs bloqueadas para uma URL especificada pelo administrador. Nesse caso, deve-se especificar a URL para qual os acessos bloqueados serão redirecionados (sem o prefixo http://) no campo abaixo.

Pasta controle de conteúdo



Analisador de URL: Esse campo especifica o agente analisador de URLs que será utilizado para categorizar as páginas da Internet. Esse agente deve ter sido previamente cadastrado no firewall. Para maiores informações veja o capítulo intitulado Cadastrando entidades.

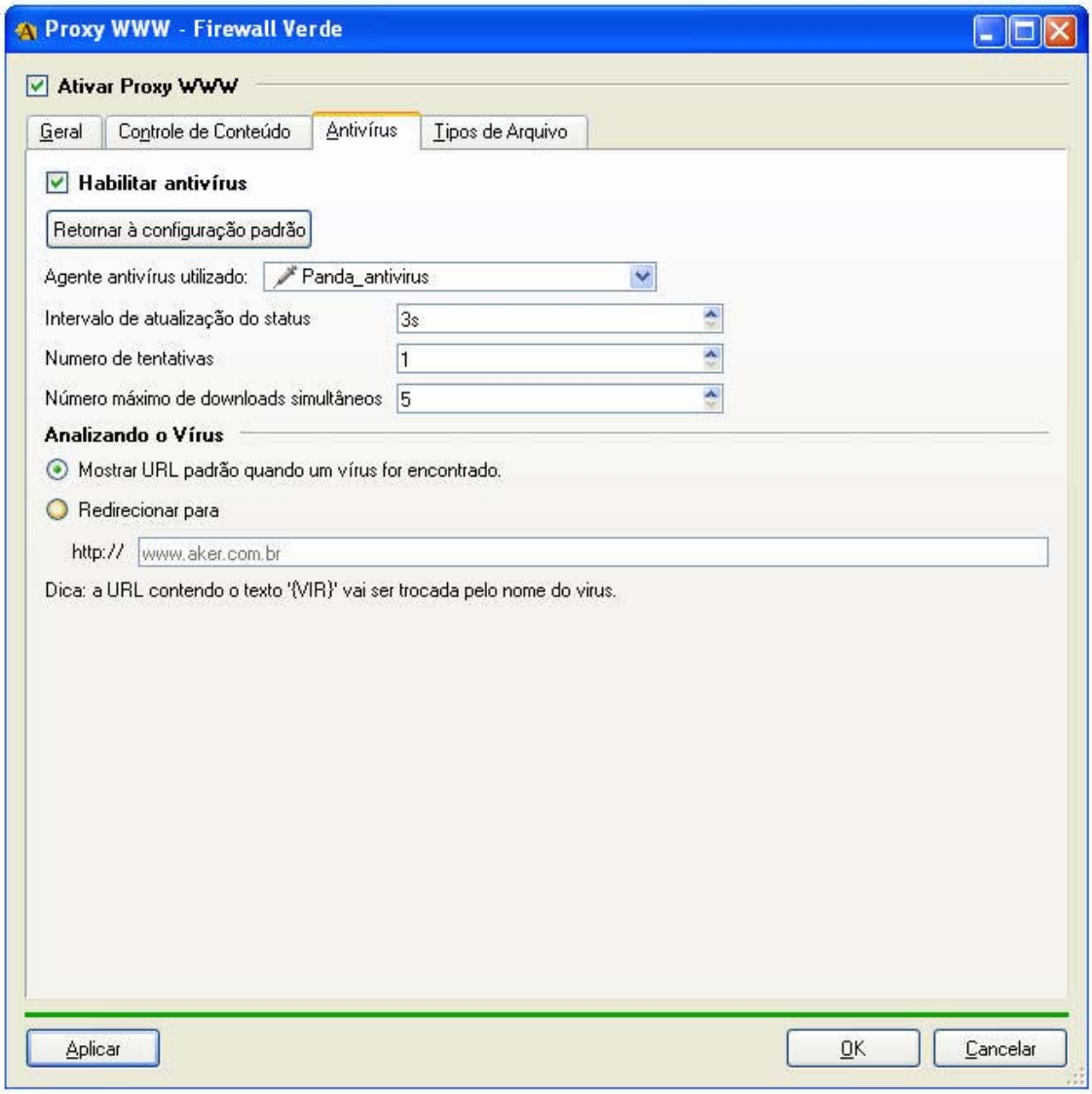
Controle SSL: Esse parâmetro permite que se defina as portas de conexão segura (https) que serão aceitas pelo firewall. Caso um cliente tente abrir uma conexão para uma porta não permitida, o firewall mostrará uma mensagem de erro e não possibilitará o acesso.

Caso se deseje utilizar apenas a porta padrão (443), deve-se selecionar a primeira opção. Essa é a configuração a ser utilizada na grande maioria dos firewalls.

A opção **Permite HTTPS para todas as portas** indica ao firewall que ele deve aceitar conexões HTTPS para quaisquer portas. Essa configuração não é recomendada para nenhum ambiente que necessite de um nível de segurança razoável, já que é possível para um usuário utilizar o proxy para acessar serviços não permitidos simulando uma conexão HTTPS.

Por último, existe a opção **Permite HTTPS para as entidades abaixo** que possibilita ao administrador definir exatamente quais portas serão permitidas. Nesse caso devem ser cadastradas as entidades correspondentes aos serviços desejados. Para maiores informações, veja o capítulo intitulado Cadastrando Entidades.

Pasta Antivírus



Habilitar antivírus: A marcação desta caixa irá permitir que o firewall faça a verificação antivírus dos conteúdos que tiverem sendo baixados.

O botão **Retornar à configuração padrão** restaura a configuração original do firewall para esta pasta.

Agente antivírus utilizado: Permite a escolha de um agente antivírus previamente cadastrado para realizar a verificação de vírus. Esse agente deve ter sido previamente cadastrado no firewall. Para maiores informações veja o capítulo intitulado Cadastrando entidades.

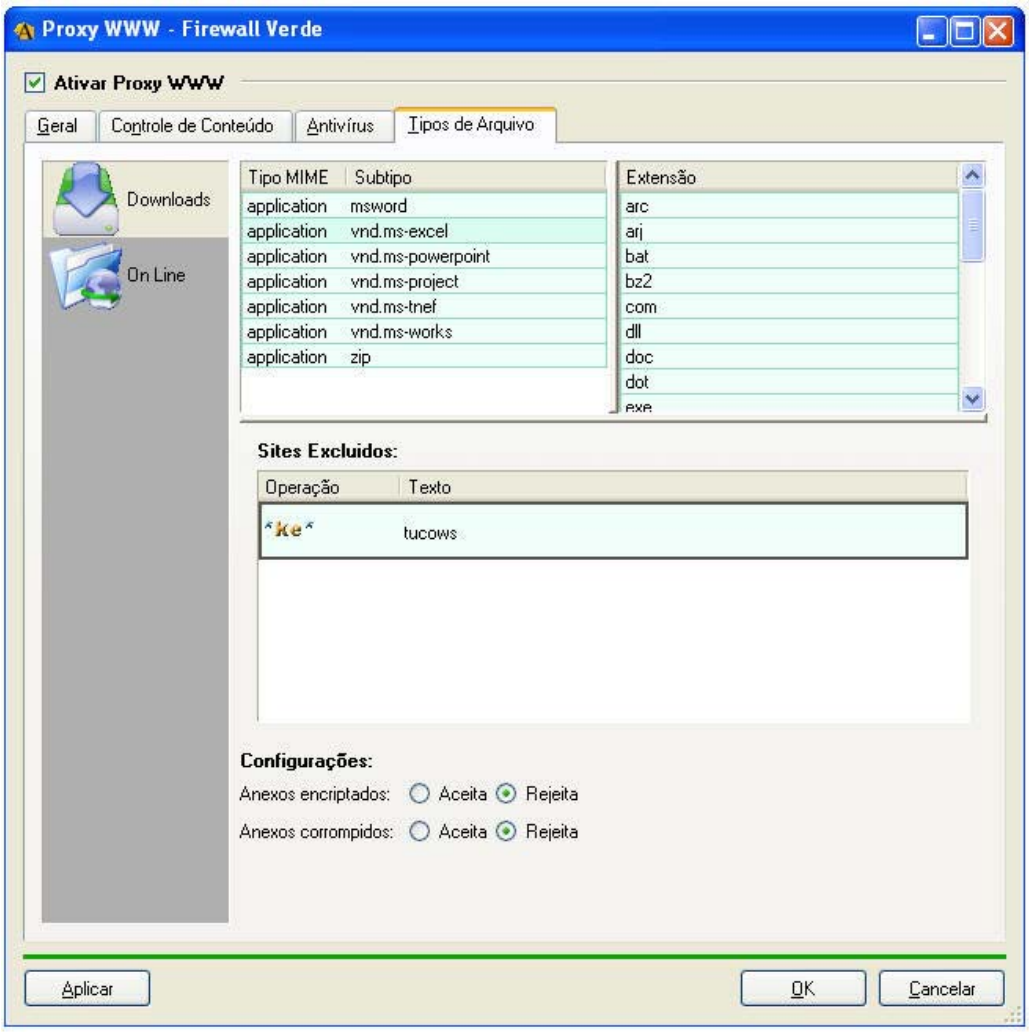
Intervalo de atualização do status: Esta opção determina o tempo em a página de download exibida pelo firewall deve ser atualizada.

Número de tentativas: Número máximo de tentativas de download para cada arquivo, caso seja necessário tentar mais de uma vez.

Número máximo de downloads simultâneos: Configura o número máximo de downloads simultâneos que o firewall irá permitir

Analisando o Vírus: Opção para mostrar uma página caso seja encontrado um vírus durante a análise do antivírus. A página poderá ser a do próprio firewall ou personalisada pelo usuário. É possível personalizar a mensagem para cada tipo de vírus encontrado, bastando utilizar a string {VIR} que será substituída pelo nome do vírus.

Pasta tipos de arquivos



- Opção **Downloads**

Esta opção serve para se especificar os arquivos que serão analisados contra vírus pelo *Download manager* do Firewall Aker, ou seja, para os quais o firewall mostrará ao usuário uma página web com o status do download do arquivo e realizará seu download em background. Esta opção é interessante para arquivos potencialmente grandes (arquivos compactados, por exemplo) ou para arquivos que normalmente não são visualizáveis de forma on-line pelo navegador.

É possível se utilizar dois critérios complementares para se decidir se um arquivo transferido deve ser analisado: a **extensão** do arquivo e seu **tipo MIME**. Se um destes

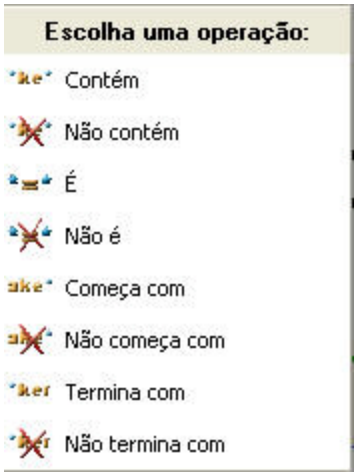
critérios for atendido, em outras palavras, se a extensão do arquivo estiver entre aquelas a serem analisadas ou o tipo MIME da mensagem estiver entre aqueles a serem analisados, então o arquivo deverá ser analisado pelo firewall.

O tipo MIME é usado para indicar o tipo de dado que está no corpo de uma resposta em um protocolo HTTP. Ele consiste em dois identificadores, o primeiro indica o tipo e o segundo indica o subtipo. O navegador usa esta informação para decidir como mostrar a informação que ele recebeu, do mesmo modo como o sistema operacional usa a extensão do nome do arquivo.

Sites Excluídos:

Deve-se escolher a operação e o texto a ser incluído para análise. Sites que se enquadrarem na lista de excluídos não serão analisados.

As escolhas dos operadores podem ser vistas abaixo:



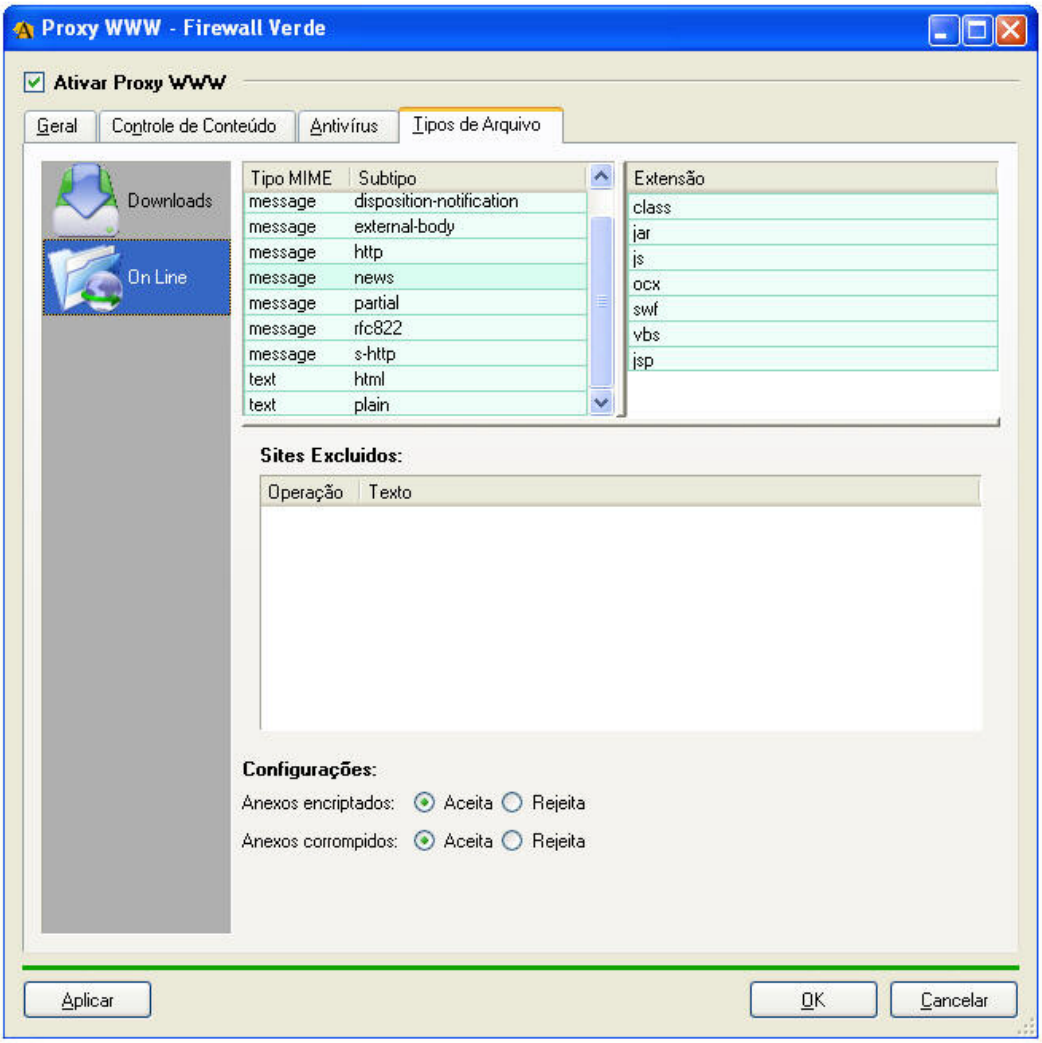
Configurações:

Anexos Encriptados: Deve-se escolher entre aceitar ou rejeitar um anexo encriptado

Anexos Corrompidos: Deve-se escolher entre aceitar ou rejeitar um anexo corrompidos

- Opção **Online**

Da mesma maneira que em downloads o administrador do firewall deve escolher os tipos MIME e as extensões. Na configuração padrão do firewall é cadastrados os seguintes tipos conforme a figura abaixo:



As demais opções são análogas ao downloads.

27-0 Configurando o proxy SOCKS

Neste capítulo mostraremos para que serve e como configurar o proxy SOCKS

27-1 Planejando a instalação

O que é o proxy SOCKS do Firewall Aker?

O proxy SOCKS é um programa especializado do Firewall Aker feito para trabalhar com programas que suportem o protocolo SOCKS nas versões 4 ou 5.

Este proxy possui como função principal prover uma melhor segurança para protocolos passarem através do firewall, principalmente protocolos complexos que utilizam mais de uma conexão. É possível através do uso do SOCKS 5 realizar autenticação de usuários para quaisquer serviços que passem pelo firewall, mesmo sem o uso do cliente de autenticação.

Ele é um proxy não transparente (para maiores informações, veja o capítulo intitulado Trabalhando com proxies), desta forma, os clientes que o forem utilizar devem ter suporte para trabalhar com proxies e devem ser configurados para usá-lo.

Utilizando o proxy SOCKS

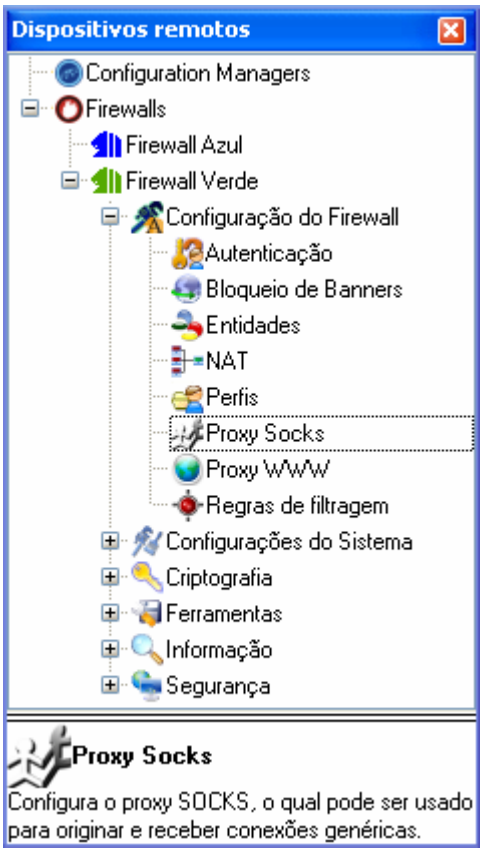
Para se utilizar o proxy SOCKS do Firewall Aker, é necessário a seguinte seqüência de passos:

1. Cria-se os perfis de acesso desejados e os associa-se com os usuários e grupos desejados. Isso foi descrito no capítulo chamado Perfis de acesso de usuários)
2. Edita-se os parâmetros de configuração do proxy SOCKS (isso será mostrado no tópico chamado Editando os parâmetros do proxy SOCKS).
3. Cria-se uma regra de filtragem possibilitando que as máquinas clientes tenham acesso ao proxy (para maiores informações, veja o capítulo intitulado O Filtro de Estados).

O proxy SOCKS do Firewall Aker escuta conexões na porta 1080, utilizando o protocolo TCP. Caso seja necessário, pode-se alterar este valor para qualquer porta, bastando para isso acrescentar o parâmetro **-p *porta***, onde *porta* é o número da porta que se deseje que ele escute, na hora de se iniciá-lo. Esta chamada se encontra no arquivo **/etc/firewall/rc.aker**, e deve ser alterada de **/etc/firewall/fwsocksd** para **/etc/firewall/fwsocksd -p 8080**, por exemplo.

27-2 Editando os parâmetros do Proxy SOCKS

Para se utilizar o proxy SOCKS, é necessário a definição de alguns parâmetros que determinarão características básicas de seu funcionamento. Esta definição é feita na janela de configuração do proxy SOCKS. Para acessá-la, basta:



- Clicar no menu *Configuração do Firewall* da janela de administração
- Selecionar o item *Proxy Socks*

A janela de configuração de parâmetros do proxy SOCKS

- O botão **OK** fará com que a janela de configuração do proxy SOCKS seja fechada e as alterações salvas
- O botão **Aplicar** enviará para o firewall todas as alterações feitas porém manterá a janela aberta

- O botão **Cancelar**, fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.

Significado dos parâmetros:
Autentica usuários SOCKS: Este campo ativa ou não a autenticação de usuários do proxy SOCKS. Caso ele esteja marcado, será solicitada ao usuário uma identificação e uma senha todas as vezes que ele tentar iniciar uma sessão e esta somente será iniciada caso ele seja autenticado por algum dos autenticadores.

Caso o usuário esteja utilizando o Cliente de Autenticação Aker e esteja com uma sessão estabelecida com o Firewall, então não será solicitado nome nem senha, ou seja, o proxy se comportará como se não estivesse realizando autenticação de usuários, mas ele está de fato fazendo-o. Se a sessão do Cliente de Autenticação for finalizada, então o proxy solicitará um nome de usuário e senha no próximo acesso. Para maiores informações sobre o Cliente de Autenticação Aker, leia o capítulo O cliente de autenticação Aker).

A versão 4 do protocolo SOCKS não permite que se realize autenticação de usuários, dessa forma, a única maneira de se autenticar clientes utilizando essa versão do protocolo é com o uso do cliente de autenticação. Caso essa opção esteja marcada, a versão suportada pelo cliente for a 4 e não existir uma sessão de perfil de acesso ativa, então o firewall não permitirá acessos para o cliente.

Tempo limite de resposta: Este parâmetro define o tempo máximo, em segundos, que o proxy aguarda por dados do cliente, a partir do momento que uma nova conexão for estabelecida. Caso este tempo seja atingido sem que o cliente envie os dados necessários, a conexão será cancelada.

Número máximo de processos: Este campo define o número máximo de processos do proxy SOCKS que poderão estar ativos simultaneamente. Como cada processo atende uma única conexão, este campo também define o número máximo de requisições que podem ser atendidas simultaneamente.

28-0 Configurando o proxy RPC

Neste capítulo será mostrado como configurar o proxy RPC

O que é o proxy RPC ?

O proxy RPC é um programa especializado do Firewall Aker feito para trabalhar com o protocolo RPC, mais especificamente, o SUN RPC, descrito na RFC1050. A sua função básica é fazer chamadas a funções remotas (*Remote Procedure Call*), ou seja, funções disponibilizadas por outras máquinas acessíveis através do firewall. Exemplos de protocolos que usam o RPC são o portmapper e o NFS.

Quando um cliente deseja realizar uma chamada RPC para um determinado número de processo, o firewall verifica a ação relacionada àquele processo. Se permitir, o proxy insere as regras de liberação de portas direta e automaticamente no kernel. Caso contrário, o firewall bloqueia o processo como se ele estivesse indisponível.

Ele é um proxy transparente (para maiores informações veja o capítulo intitulado Trabalhando com proxies), desta forma, nem o servidor nem o cliente sabem de sua existência.

Utilizando o proxy RPC

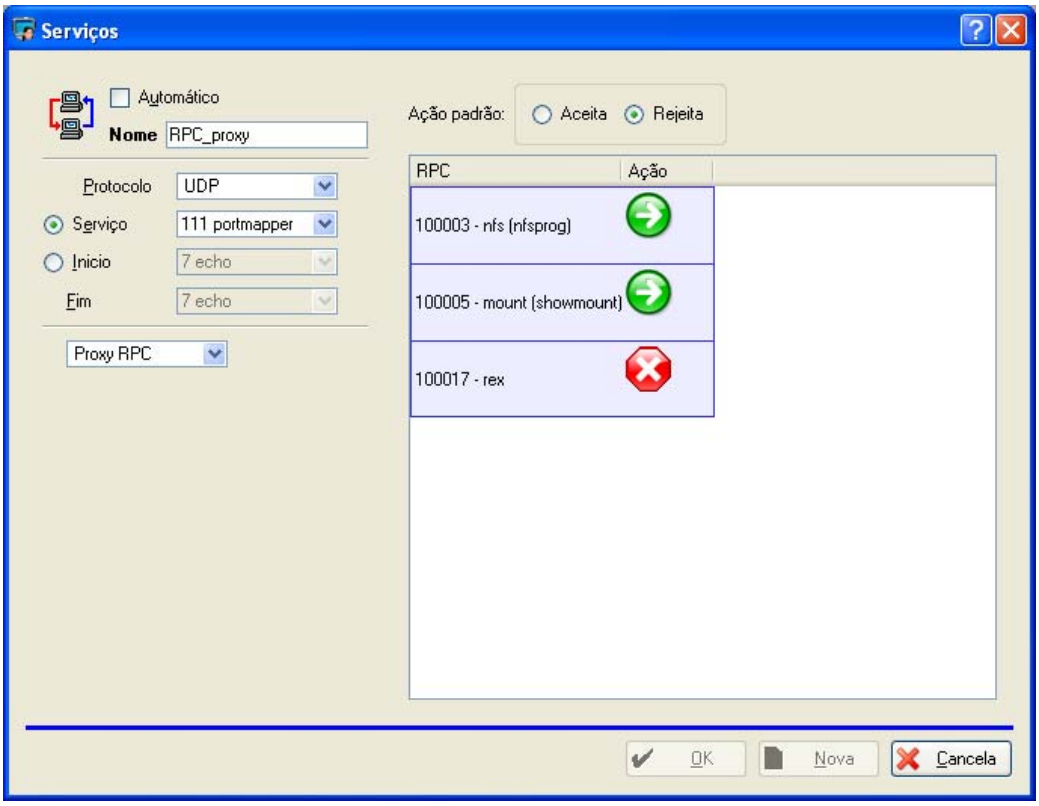
Para utilizar o proxy RPC, é necessário executar uma seqüência de 2 passos:

1. Criar um serviço que será desviado para o proxy RPC e editar os parâmetros do contexto a ser usado por este serviço (para maiores informações, veja o capítulo intitulado Cadastrando Entidades)
2. Acrescentar uma regra de filtragem permitindo o uso do serviço criado no passo 1, para as redes ou máquinas desejadas (para maiores informações, veja o capítulo intitulado Filtro de Estados)

28-1 Editando os parâmetros de um contexto RPC

A janela de propriedades de um contexto RPC será mostrada quando se selecionar o protocolo **UDP** e a opção **Proxy RPC** na janela de edição de serviços. Através dela é possível definir o comportamento do proxy RPC quando este for lidar com o serviço em questão.

A janela de propriedades de um contexto RPC

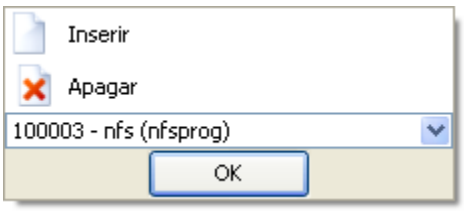


Na janela de propriedades são configurados todos os parâmetros de um contexto associado a um determinado serviço. Ela consiste dos seguintes campos:

Ação padrão: Este campo indica a ação que será aplicada a todos os serviços remotos que não estiverem presentes na lista de permissões. O valor *aceita* permite que o serviço seja utilizado e o valor *rejeita* impede sua utilização.

Lista de permissões: Esta lista define, de forma individual, as permissões de acesso aos serviços remotos.

> Para executar qualquer operação sobre um serviço na lista de permissões, basta clicar com o botão direito do mouse sobre ele na coluna **RPC**. Aparecerá o seguinte menu (Caso não exista nenhum serviço selecionado, somente as opções *Inserir* e *Apagar* estarão presentes):



- **Inserir:** Esta opção permite incluir um novo serviço na lista. Se algum serviço estiver selecionado, o novo será inserido na posição selecionada. Caso contrário, o novo serviço será incluído no final da lista.
- **Apagar**: Esta opção remove da lista o serviço selecionado.
- **Lista de serviços**: Contém uma lista pré-definida de serviços e seus respectivos números. É possível acrescentar serviços que não estejam presentes nessa lista.

Para isso, basta clicar no campo logo abaixo da opção *Apagar* e digitar o código do novo serviço.

Para alterar a ação aplicada a um serviço, basta clicar com o botão direito do mouse sobre ele na coluna **Ação** e escolher uma das opções, **Aceita** ou **Rejeita**, que aparecerão no menu seguinte:

29-0 Utilizando as Ferramentas da Interface Gráfica

Neste capítulo será mostrada a função das diversas ferramentas presentes na interface gráfica do Firewall Aker.

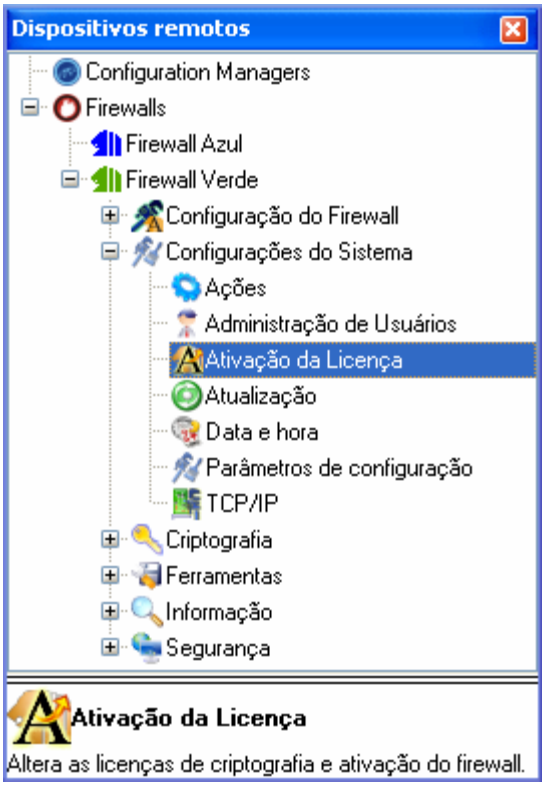
O que são as ferramentas da interface gráfica do Firewall Aker ?

As ferramentas são um conjunto de utilitários presentes apenas na interface gráfica do Firewall Aker. Elas servem para facilitar a administração do firewall, provendo uma série de funções bastante úteis no dia-a-dia.

29-1 Chaves de Ativação

Esta opção permite se atualizar a chave de ativação do Firewall Aker e a chave de licenças adicionais para clientes de criptografia.

Para se atualizar qualquer uma destas chaves através da interface gráfica, deve-se:



- Clicar no menu *Configuração do Sistema* da janela de administração do firewall
- Selecionar o item *Ativação da Licença*

A janela de atualização de chaves

Esta janelas tem dois painéis. O primeiro é usado para alterar a licença do firewall. Você não pode ver a licença antiga, mas pode ver os seus dados de expiração e quantidade de hosts internos. No segundo tab, o mesmo ocorre para o Secure Roaming.

Para se alterar qualquer uma destas chaves, basta-se digitar o valor da nova chave e clicar no botão **OK**. Assim que a digitação começa, a chave antiga desaparece e o programa permite a visualização dos caracteres digitados. Caso não se deseje atualizar a chave, deve-se clicar no botão **Cancelar**.

A barra de ferramentas possui um botão para carregar a licença a partir de um arquivo fornecido pela Aker.

O nome da empresa, o endereço IP e a(s) chave(s) devem ser digitadas exatamente conforme fornecidos pela Aker Security Solutions ou seu representante autorizado. No campo empresa, letras maiúsculas e minúsculas são consideradas diferentes.

Caso a chave recém atualizada possua parâmetros distintos da chave anterior (como por exemplo, habilitação da criptografia ou alterações no número de licenças de clientes de criptografia), é necessário se finalizar a sessão de administração remota e se conectar novamente no firewall para que a interface perceba a mudança nestes parâmetros.

29-2 Salvar configurações

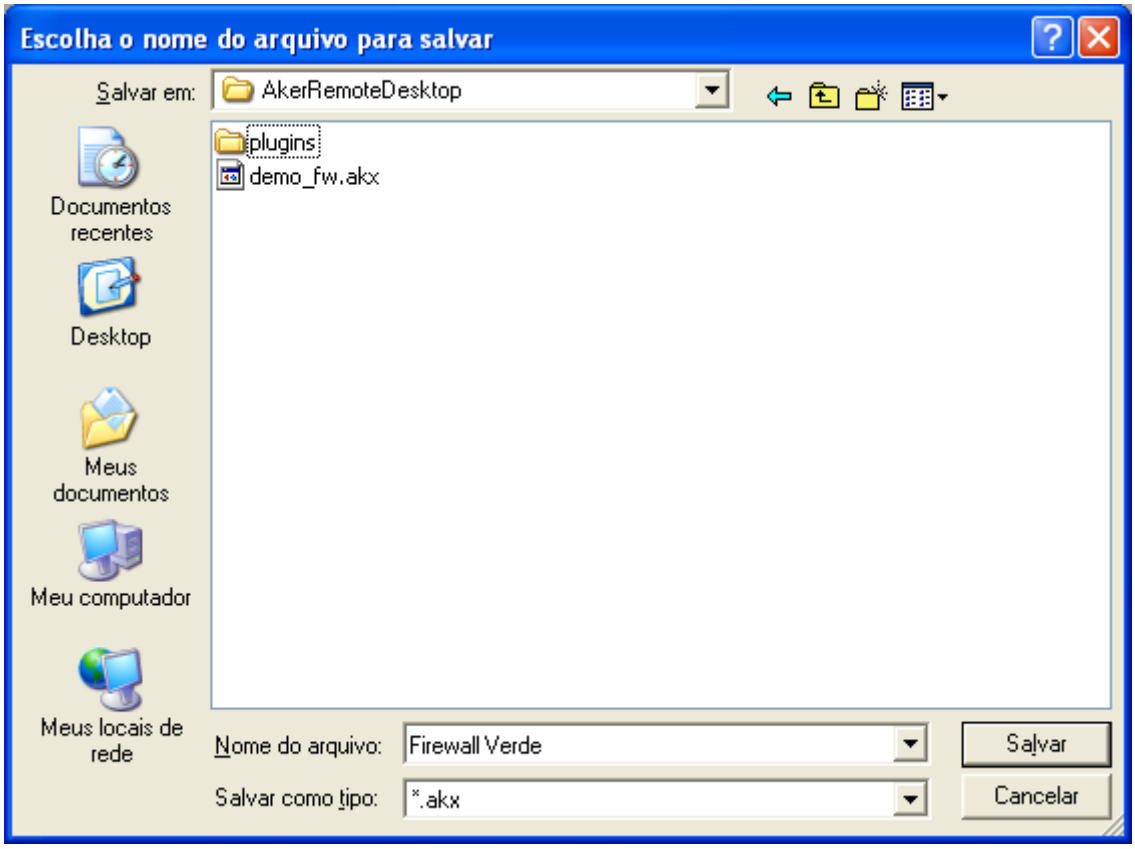
Esta opção permite salvar a configuração completa do firewall na máquina onde se está administrando. No caso de algum desastre, pode-se facilmente restaurar esta configuração posteriormente.

Para se realizar uma cópia de segurança, deve-se:

- Clicar no firewall para o qual será salva a cópia de segurança
- Selecionar a opção *Salvar configurações* na barra de ferramentas ou no menu com o nome do firewall selecionado

---

A janela para salvar configurações:



Após se digitar o nome do arquivo salvo, deve-se clicar no botão **Salvar**.. Caso não se deseje mais gravar a cópia de segurança, basta clicar no botão **Cancelar**.

29-3 Carregar configurações

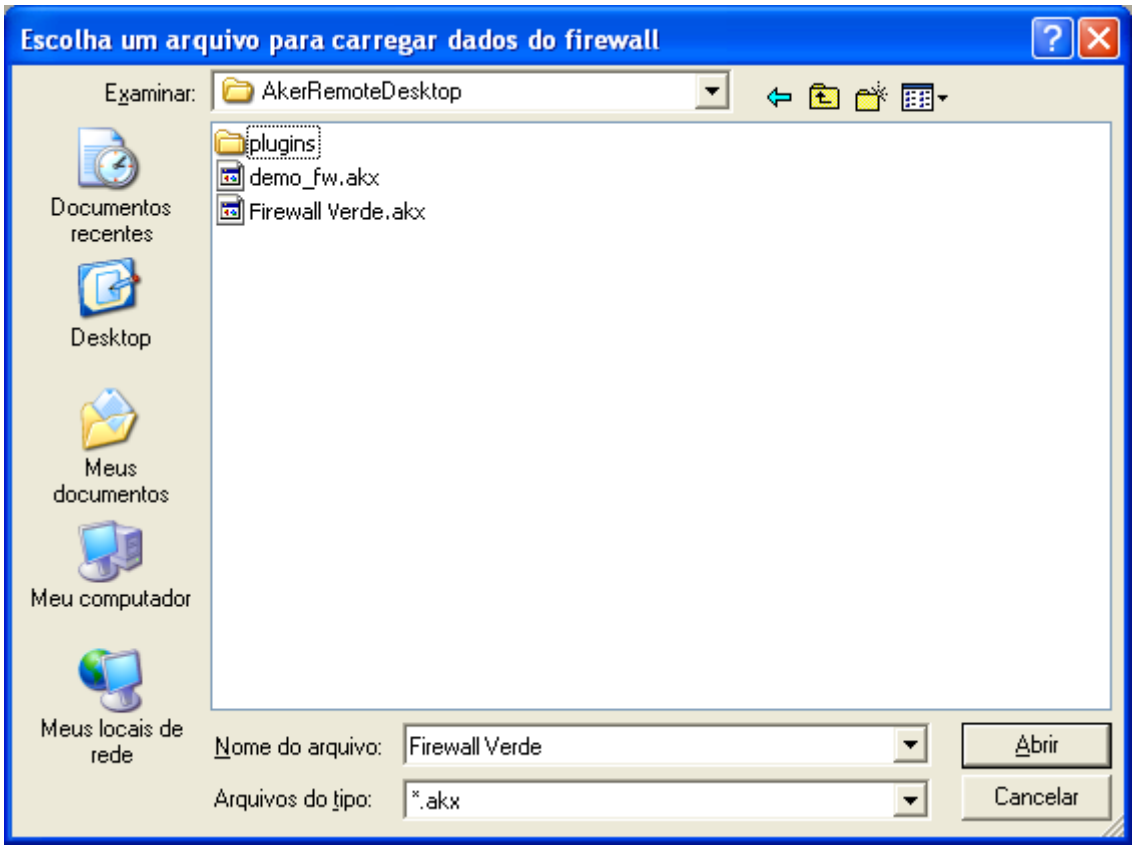
Esta opção permite se restaurar a cópia de segurança da configuração completa do firewall realizada através da opção anterior.

Para se restaurar uma cópia de segurança, deve-se:

- Clicar no firewall para o qual será carregada a cópia de segurança
- Selecionar o item *Carregar configurações* na barra de ferramentas ou no menu com o nome do firewall selecionado

---

A janela para carregar configurações:



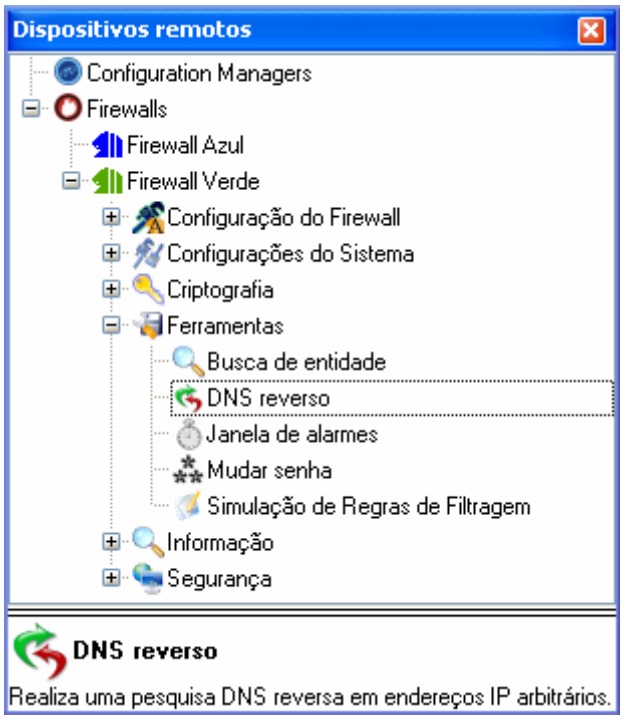
Esta janela permite que se escolha o nome do arquivo de onde a configuração será restaurada. Após seu nome ser especificado, o firewall lerá todo seu conteúdo, fará vários testes de consistência e se o seu conteúdo estiver válido será carregado.

- O botão **Abrir** fará com que a cópia seja carregada e a configuração do firewall imediatamente atualizada.
- O Botão **Cancelar** fará com que a janela seja fechada porém a cópia de segurança não seja carregada

29-4 DNS Reverso

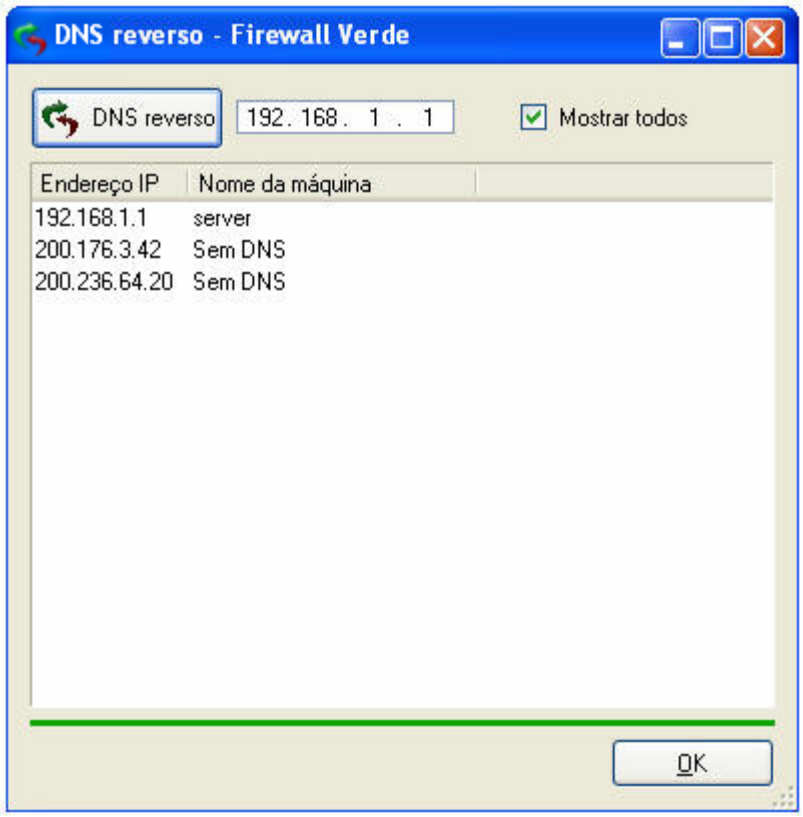
DNS reverso é utilizado para se resolver nomes de máquinas a partir de endereços IP. A janela de resolução de DNS reverso do Firewall Aker serve para prover resolução de endereços sem a necessidade de utilização de programas adicionais.

Para ter acesso a janela de resolução de DNS reverso, basta:



- Clicar no menu *Ferramentas* da janela de administração do firewall
- Selecionar o item *DNS Reverso*

A janela de resolução de DNS reverso



Esta janela consiste de um campo para se digitar o endereço IP que se deseja resolver e uma lista com os endereços IP já resolvidos anteriormente.

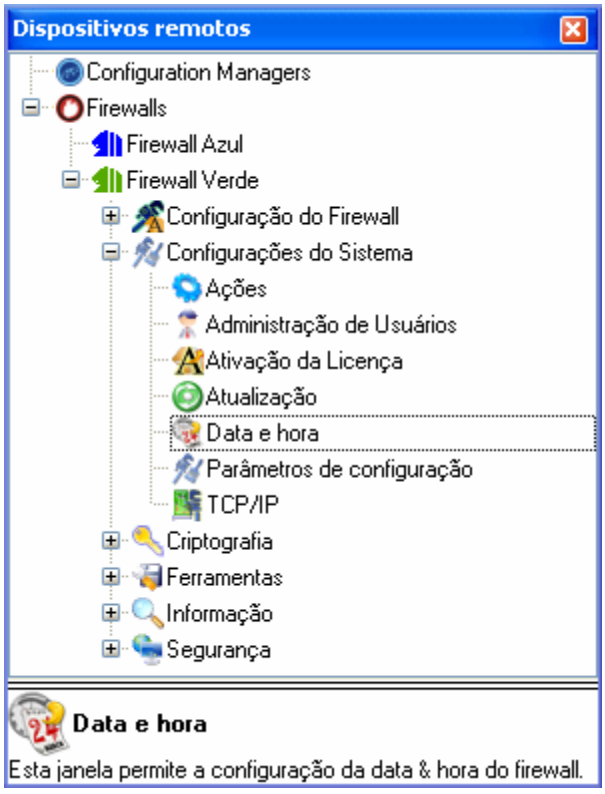
- O botão **OK** fará com que a janela seja fechada.
- A opção **Mostrar todos**, se estiver marcada, fará com que sejam mostrados todos os endereços já resolvidos na lista na parte inferior da janela.

Para se resolver um endereço, deve-se digitá-lo no campo e pressionar o botão **DNS Reverso**. Neste momento o endereço será mostrado na lista na parte inferior da janela, junto com o *status* da resolução. Após algum tempo, será mostrado o nome da máquina correspondente ao endereço ou uma indicação de que o endereço informado não possui DNS reverso configurado.

29-5 Data e Hora

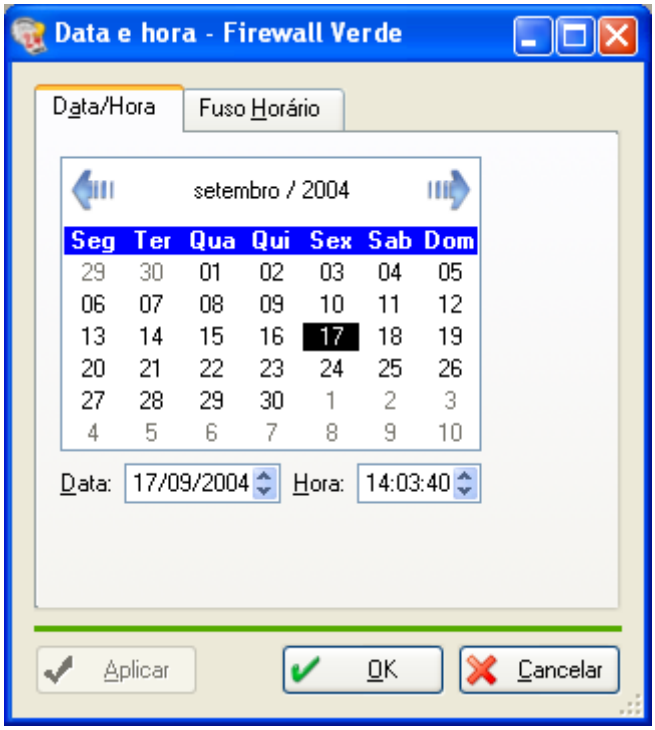
Esta opção permite ao administrador verificar e alterar a data e a hora do firewall. A data e hora configuradas corretamente são essenciais para o funcionamento da tabela de horário das regras e dos perfis de acesso WWW, das trocas de chaves através do protocolo SKIP e dos sistema de log e eventos.

Para ter acesso a janela de configuração de data e hora, basta:



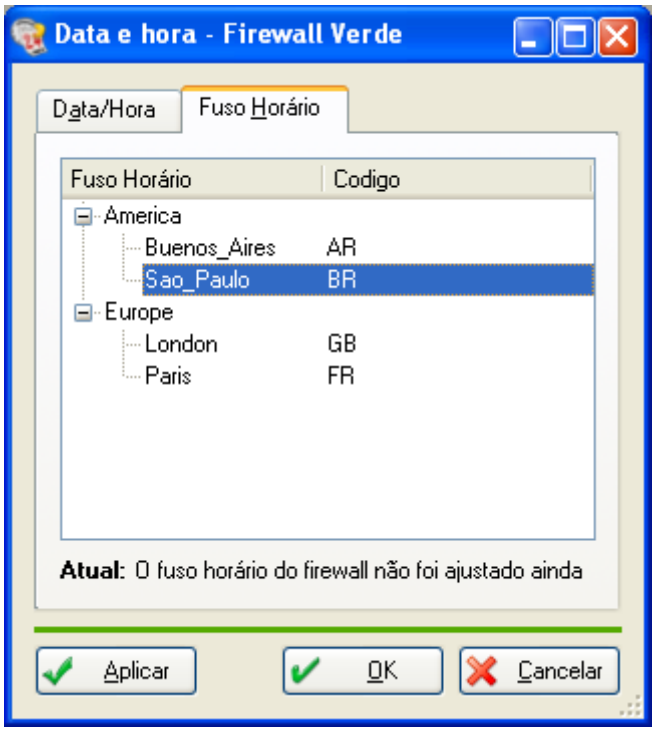
- Clicar no menu *Configurações do Sistema* da janela de administração do firewall
- Selecionar o item *Data e Hora*

A pasta de data e hora


Data e hora - Firewall Verde
Data/Hora
Fuso Horário
setembro / 2004
Seg Ter Qua Qui Sex Sab Dom
29 30 01 02 03 04 05
06 07 08 09 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 1 2 3
4 5 6 7 8 9 10
Data: 17/09/2004
Hora: 14:03:40
Aplicar
OK
Cancelar

Esta janela consiste de dois campos que mostram o valor da data e hora configurados no firewall. Para se alterar qualquer um destes valores, basta se colocar o valor desejado no campo correspondente. Para escolher o mês pode-se usar as setas de navegação.

A pasta de Fuso Horário



Escolha o fuso horário que mais se aproxima da região aonde o firewall será instalado.

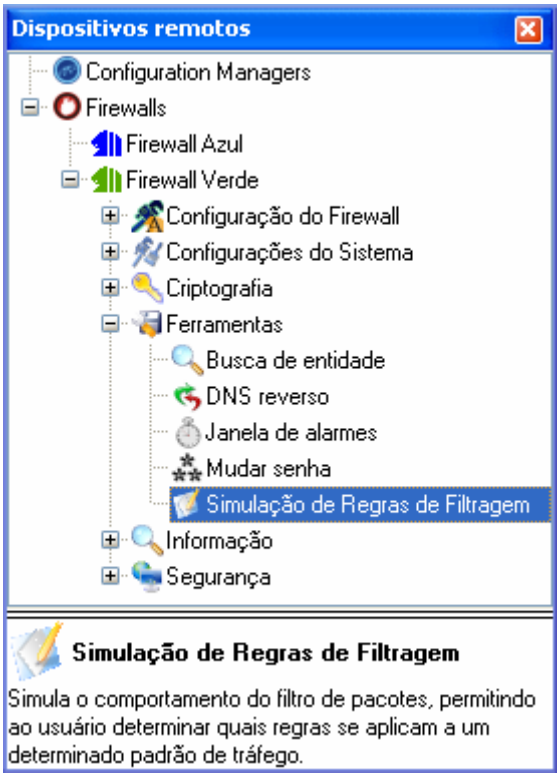
- O botão **Aplicar** alterará a data e hora e manterá a janela aberta.

- O botão **OK** fará com que a janela seja fechada e as alterações salvas.
- O botão **Cancelar** fechará a janela e descartará as modificações efetuadas.

29-6 Simulação de Regras de Filtragem

As varreduras de regras permitem ao administrador testar a configuração das regras de filtragem do firewall através de uma simulação de tentativas de conexões. Ao analisar o resultado desta simulação, é possível se verificar se o firewall está realmente bloqueando as conexões que não devem ser aceitas e permitindo a passagem das que devem.

Para ter acesso a janela de varreduras, basta:



- Clicar no menu *Ferramentas* da janela de administração do firewall
- Selecionar o item *Simulação de regras de filtragem*

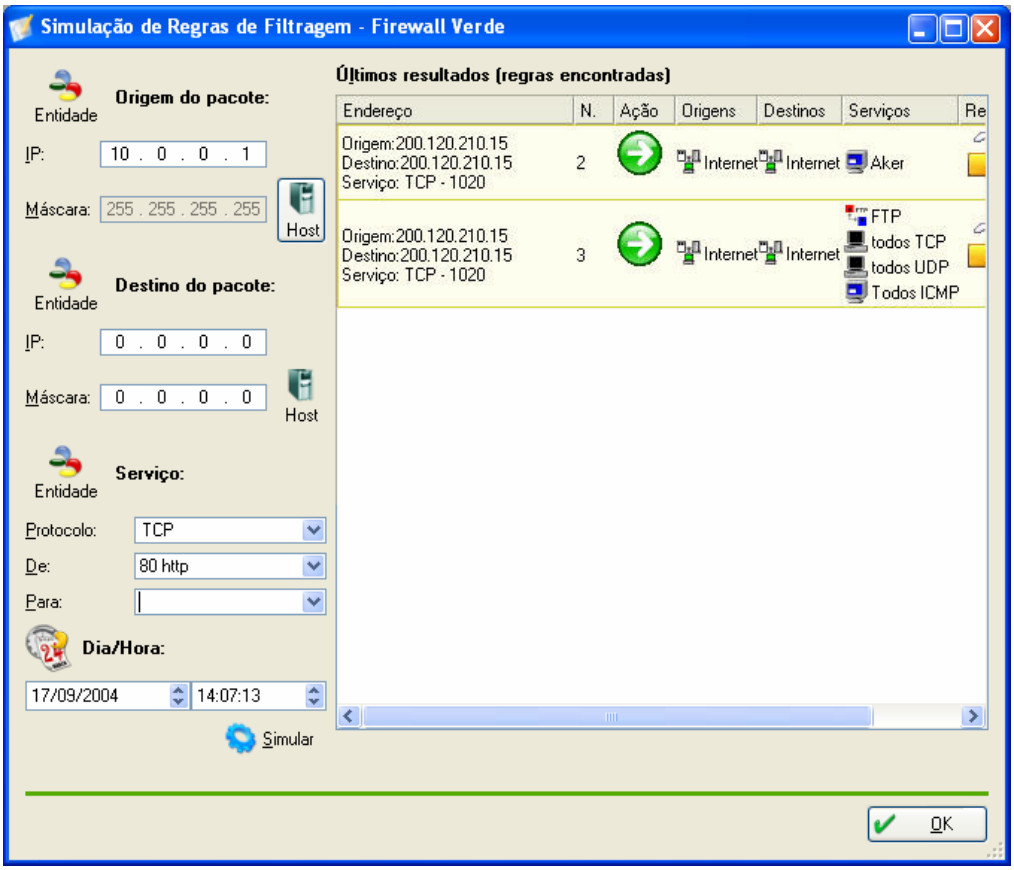
A janela de varredura de regras

É possível se alternar entre a varredura por endereços IP ou por entidades. A varredura por entidades é útil quando já se tem cadastradas no sistema todas as máquinas, redes e serviços que serão utilizados. A varredura por IP é mais indicada quando se deseja utilizar máquinas, redes ou serviços que não estão cadastrados e que não se deseja cadastrar (por exemplo, máquinas externas que não serão utilizadas em nenhuma regra de filtragem).

É possível se selecionar para origem, destino e serviços, indepentendemente, se devem ser utilizadas entidades ou não. Para alternar entre os dois modos de operação basta se clicar nos ícones correspondentes à esquerda de cada um destes campos.

- **Varredura por IP**

Quando a opção **Varrer por IP** estiver selecionada, a janela de varreduras terá o seguinte formato:



Os campos **IP** e **Máscara**, dentro de Origem do Pacote, permitem que se especifique a faixa de máquinas a serem utilizadas como origem das conexões simuladas. Os campos **IP** e **Máscara**, dentro de Destino do Pacote especificam a faixa de máquinas a serem utilizadas como destino.

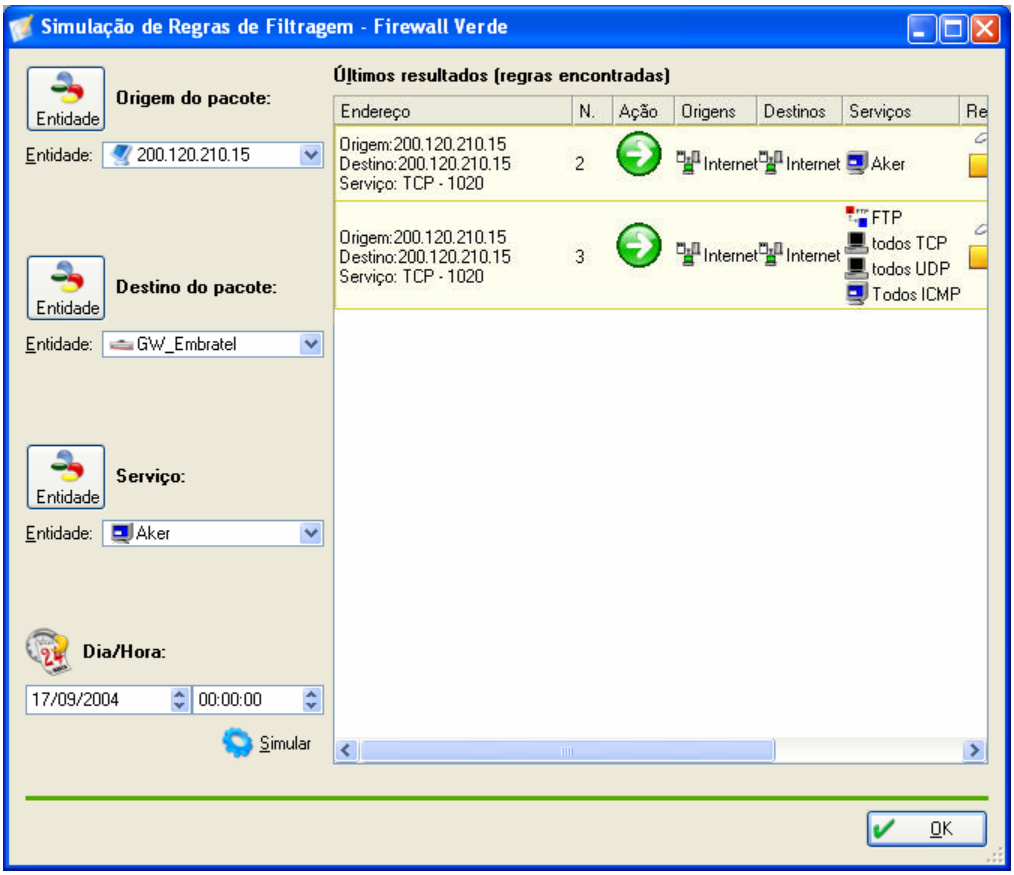
O campo **Serviço** permite que se especifique o protocolo e a faixa de portas a serem simuladas.

No caso dos protocolos TCP e UDP, os valores dos serviços são as portas destino; no caso do ICMP são o tipo de serviço e no caso de outros protocolos o valor do protocolo.

O campo **Dia/Hora** permite que o adminstrador teste as regras para uma determinada hora e dia da semana.

- **Varredura por Entidades**

Quando a opção **Varrer por Entidades** estiver selecionada, a janela de varreduras terá o seguinte formato:



O campo **Origem do pacote** permite que se especifique a entidade que será usada na origem das conexões simuladas. O campo **Destino do pacote** especifica para qual entidade as conexões simuladas devem se dirigir.

O campo **Serviço** permite que se especifique o protocolo e a faixa de portas a serem simuladas, através de uma entidade.

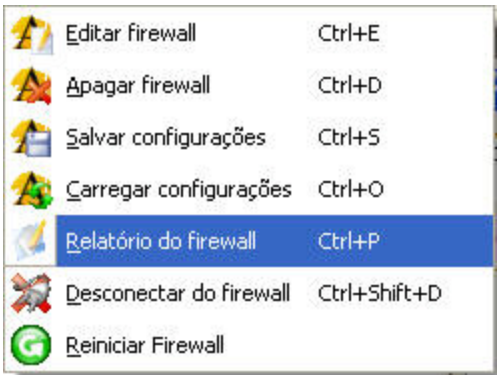
O campo **Dia/Hora** permite que o adminstrador teste as regras para uma determinada hora e dia da semana.

Só é possível se selecionar uma entidade como origem, uma como destino e um serviço.

29-7 Relatórios

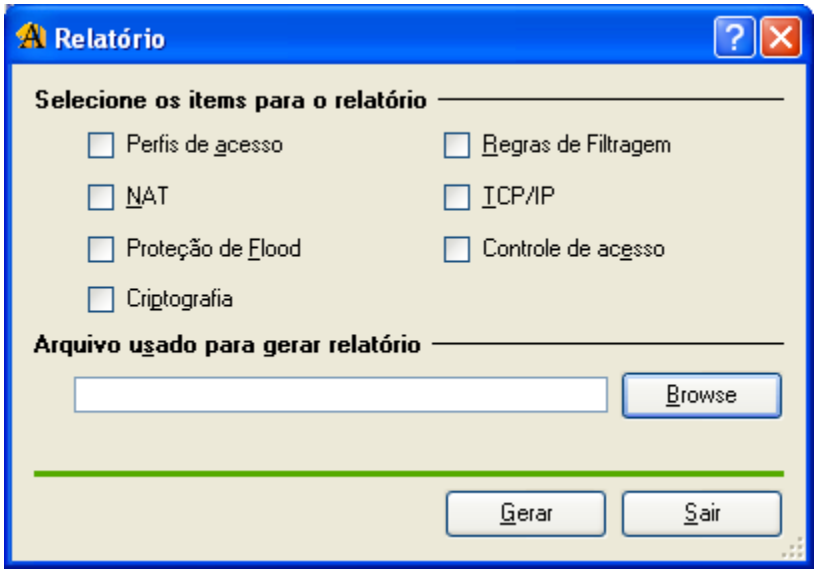
Esta opção possibilita que o administrador imprima um relatório de toda (ou de parte) da configuração do firewall de forma fácil e rápida. Este relatório é bastante útil para fins de documentação ou de análise da configuração.

Para ter acesso a janela de relatórios basta:



- Clicar no firewall para o qual se deseja gerar o relatório
- Selecionar o item *Relatório do firewall* no menu com o mesmo nome do firewall selecionado.

A janela de relatórios



Esta janela consiste de várias opções distintas, uma para cada parte da configuração do firewall, que podem ser selecionadas independentemente. Para se gerar um relatório, deve-se proceder da seguinte forma:

1. Marca-se os itens que se deseja imprimir
2. Clica-se no botão **Procurar** e escolha o diretório onde irão ser armazenadas as páginas html.
3. Abra o diretório e selecione o arquivo html para imprimir seu relatório.

Caso se deseje cancelar a emissão do relatório, basta clicar no botão **Cancelar**.

29-8 Atualizações

O que são atualizações e onde consegui-las ?

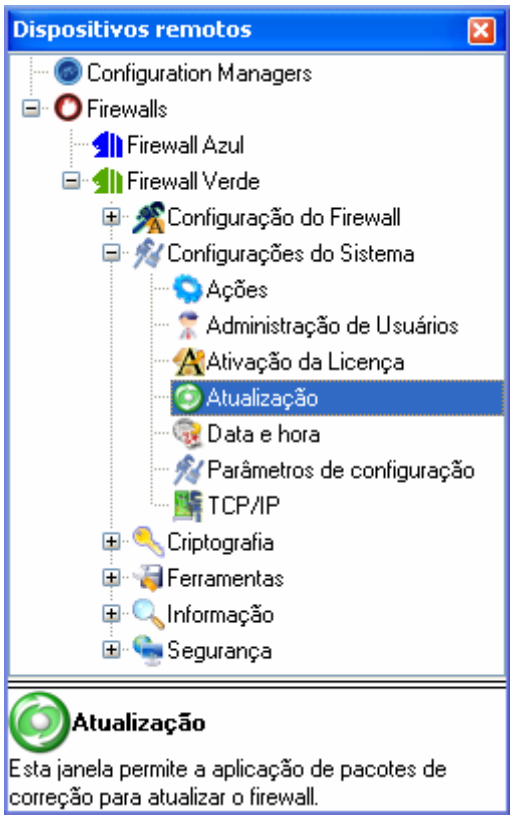
Como todo o software, o Firewall Aker pode eventualmente apresentar bugs em seu funcionamento. À medida em que estes problemas são resolvidos, a Aker produz um arquivo que permite a atualização de seu firewall e a eliminação destes erros. Algumas vezes também são adicionadas determinadas características novas em uma versão já existente, de modo a aumentar sua performance ou aumentar sua flexibilidade.

Em ambos os casos, os arquivos de atualização ou correção são disponibilizados de forma gratuita no site da Aker: basta procurar o menu *Download* e selecionar a opção *Correções e Atualizações*. Estes arquivos são sempre cumulativos, ou seja, é necessário apenas baixar a última versão disponível e esta incluirá as correções presentes nos arquivos de correção/atualização anteriores.

A janela de atualizações

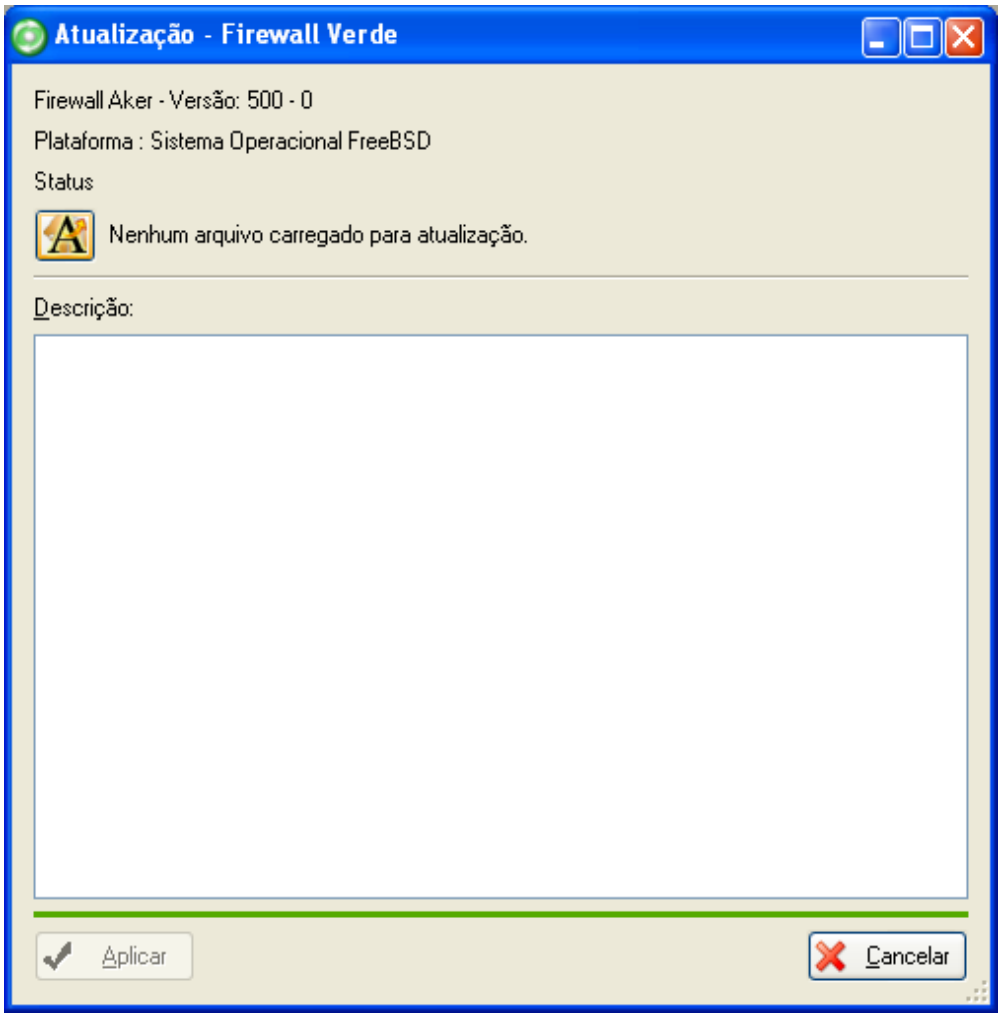
Esta opção permite que se aplique uma atualização ou correção do Firewall Aker remotamente, através da interface gráfica. É possível até mesmo atualizar completamente uma versão do firewall através desta opção.

Para se ter acesso à janela de atualizações basta:



- Clicar no menu *Configurações do Sistema* da janela de administração do firewall
- Selecionar o item *Atualização*

A janela de Atualização



Inicialmente a janela de atualizações mostrará apenas a versão do firewall, seu nível de correção e a plataforma (sistema operacional e versão) na qual o firewall está rodando.

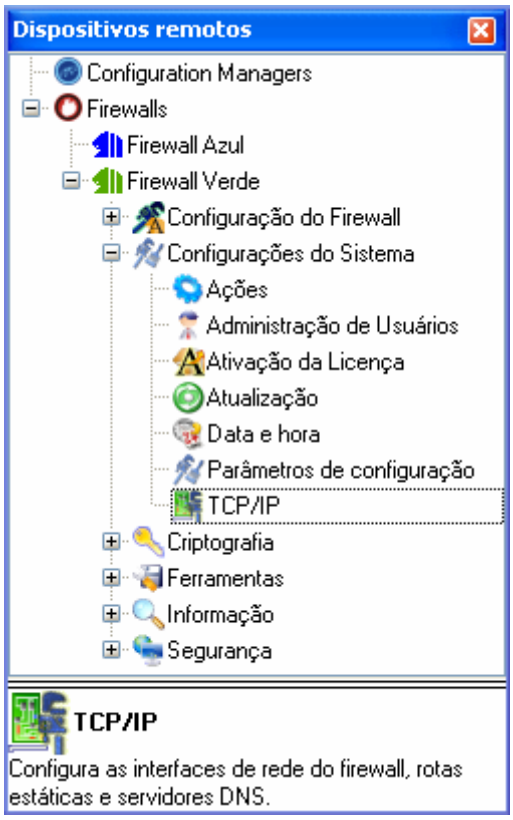
Para se aplicar uma atualização ou correção, basta se clicar no botão **Carregar arquivo de atualização**. A partir deste momento será mostrada, na parte inferior da janela, a descrição da correção ou atualização e a versão do firewall e do sistema operacional a qual ele se destina. Feito isso, basta se clicar no botão **Aplicar**, na parte inferior da janela para que a atualização ou correção seja aplicada.

Caso a atualização ou correção sejam destinadas a uma versão diferente de sistema operacional ou de versão do firewall, então o botão **Aplicar** ficará desabilitado, não permitindo sua aplicação.

29-9 Configuração TCP/IP

Esta opção permite que se configure todos os parâmetros de TCP/IP do firewall através da interface gráfica. É possível se configurar endereços de interfaces de rede, DNS e roteamento, bem como as opções de PPPoE e Servidor/Relay DHCP.

Para se ter acesso à janela de configuração TCP/IP basta:

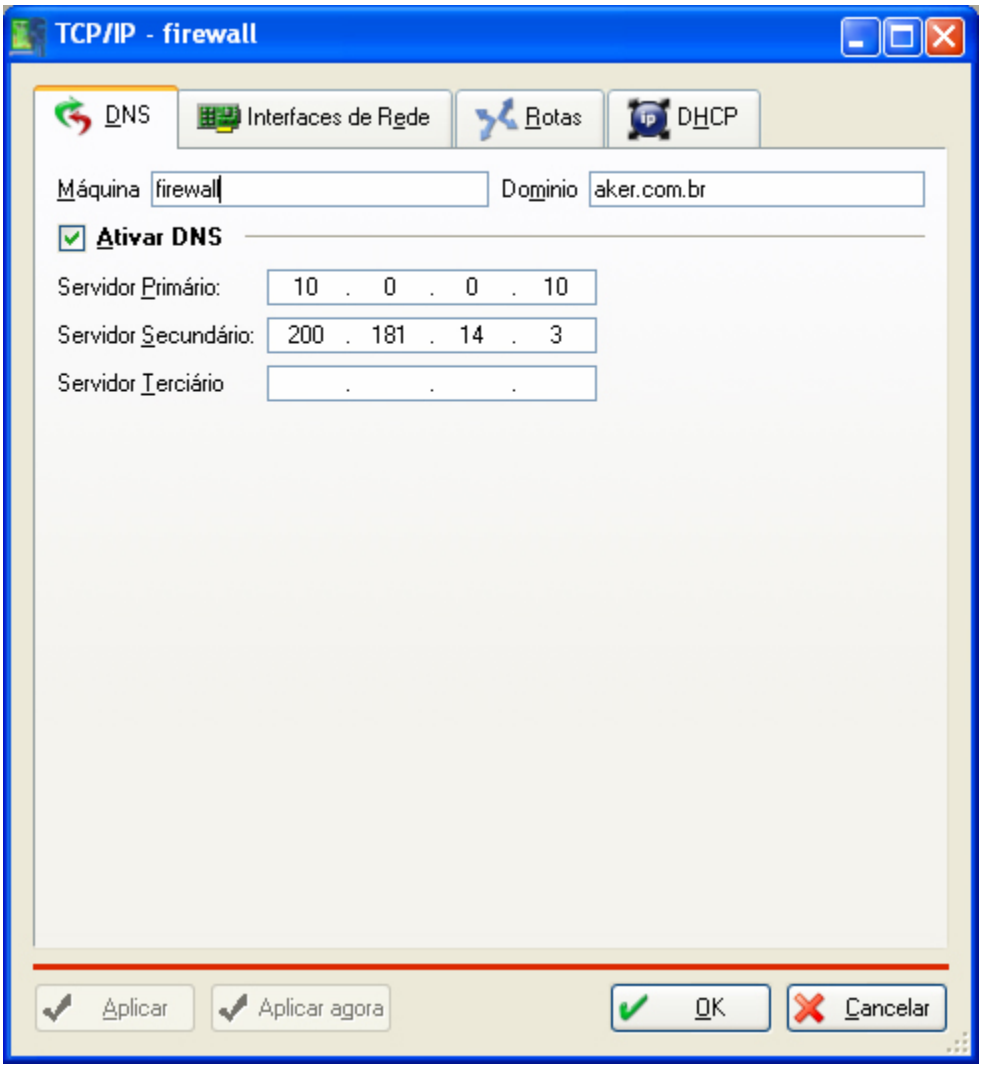


- Clicar no menu *Configurações do Sistema* da janela de administração do firewall
- Selecionar o item *TCP/IP*

A janela de configuração TCP/IP

Esta janela consiste de quatro pastas onde cada uma é responsável por um tipo de configuração diferente. São elas:

DNS



Nesta pasta são configuradas todas as opções relacionadas com a resolução de nomes ou DNS. Ela consiste dos seguintes campos:

Máquina: Nome da máquina na qual o firewall está rodando.

Domínio: Nome do domínio no qual o firewall está rodando.

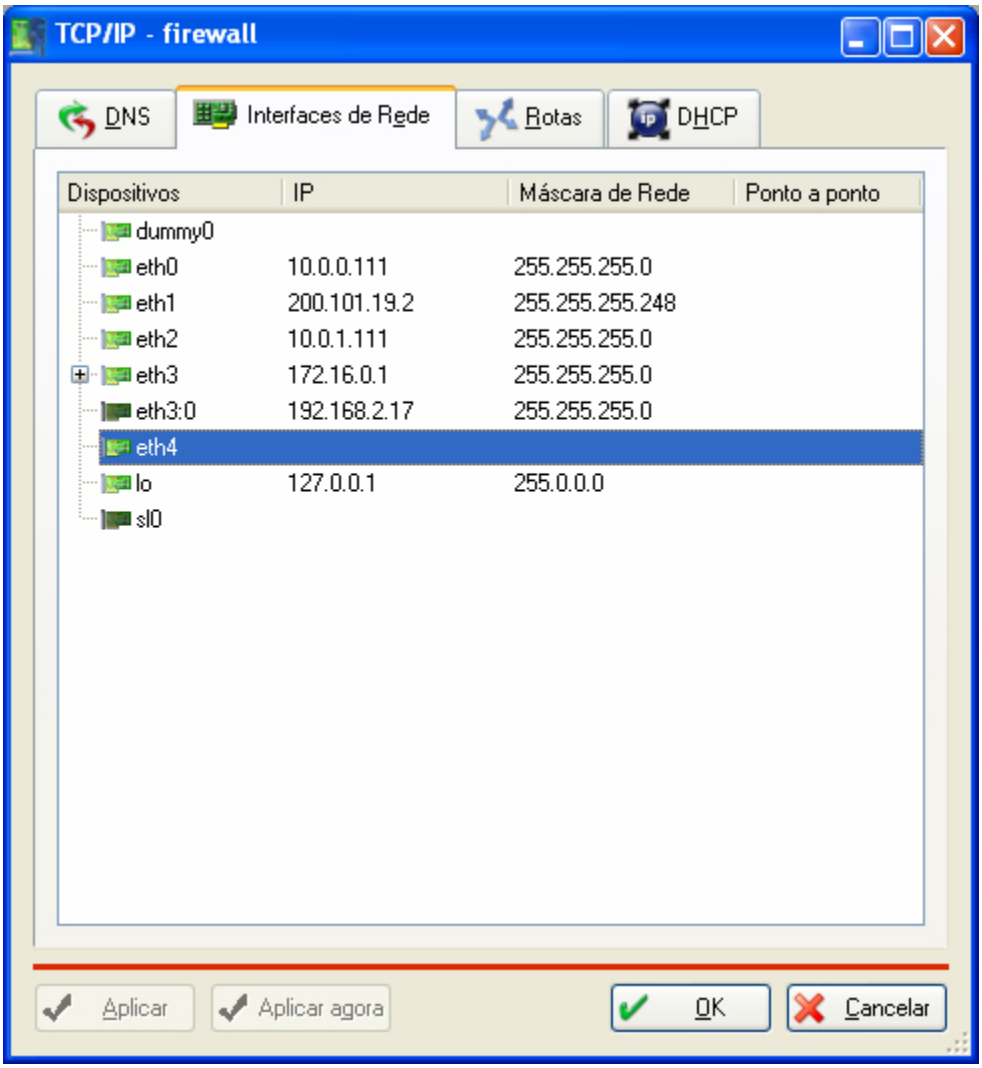
DNS Ativo: Esta opção deve ser marcada para ativar a resolução de nomes via DNS e desmarcada para desativá-la.

Servidor primário: Este campo define o servidor DNS primário que será consultado para se resolver um nome. Ele é obrigatório se a opção *DNS ativo* estiver marcada.

Servidor secundário: Este campo define o servidor DNS secundário que será consultado se o primário estiver fora do ar. Ele é opcional.

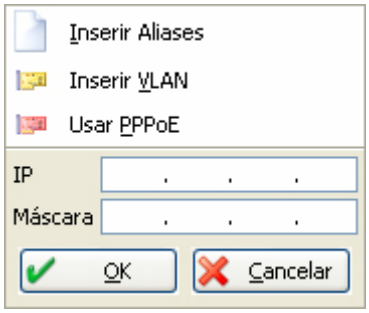
Servidor terciário: Este campo define o servidor DNS terciário que será consultado se o primário e o secundários estiverem fora do ar. Ele é opcional.

Interfaces de Rede



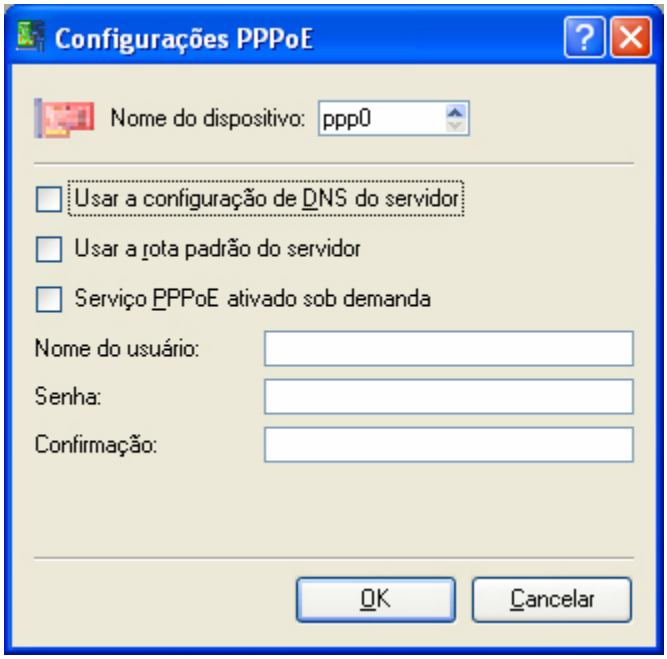
Nesta pasta pode-se configurar os endereços IP atribuídos a todas as interfaces de rede reconhecidas pelo firewall. Ela consiste de uma lista onde são mostrados os nomes de todas as interfaces e os endereços IP e máscaras de cada uma (é possível se configurar até 31 endereços distintos para cada interface). Caso uma interface não tenha um endereço IP configurado, os campos correspondentes ao endereço e à máscara serão mostrados em branco.

Para se configurar ou modificar o endereço IP ou máscara de uma interface, deve-se clicar sobre a entrada do dispositivo correspondente e usar o menu suspenso que irá surgir:



Neste mesmo menu pode-se atribuir um *alias* para a interface ou criar uma VLAN associada a esta interface. Uma VLAN usa o sistema de VLAN tagging (802.1q) para permitir que, com uma conexão somente ao switch, se tenha acesso a todas as suas VLANs, inclusive controlando o acesso entre elas. Para cada uma, uma interface virtual será criada dentro do Firewall.

Este menu também possui a opção **Usar PPPoE**. Esta opção permite que se defina que esta interface trabalhará com PPPoE (usado basicamente para a conexão com modems ADSL). Ao ser selecionada, a seguinte janela será mostrada:



Nome do dispositivo: Este campo indica o nome do dispositivo interno que será utilizado na comunicação PPPoE. É importante que no caso de que haja mais de uma interface trabalhando em PPPoE, que eles sejam distintos.

Usar a configuração de DNS do servidor: Se esta opção estiver marcada, o firewall utilizará como servidor de DNS o valor recebido através do PPPoE.

Usar a rota padrão do servidor: Se esta opção estiver marcada, o firewall utilizará como rota padrão o valor recebido através do PPPoE.

Serviço PPPoE ativado sob demanda: Se esta opção estiver marcada, o firewall ativará o serviço PPPoE apenas quando houver tráfico de rede direcionado através desta interface de rede.

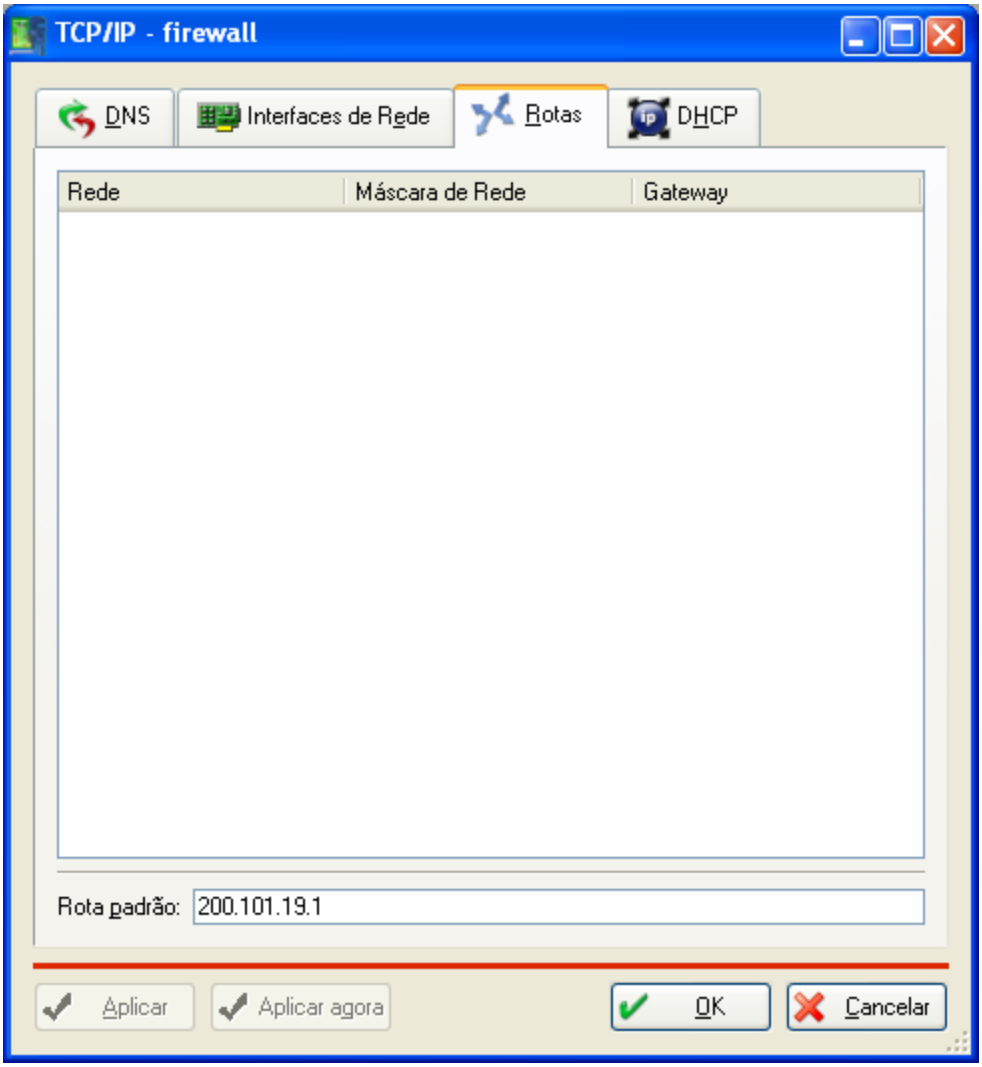
Nome do Usuário: Nome do usuário que será utilizado na autenticação durante o estabelecimento da sessão PPPoE.

Senha: Senha que será utilizada na autenticação durante o estabelecimento da sessão PPPoE.

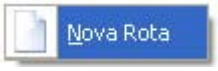
Confirmação: Confirmação da senha que será utilizada na autenticação durante o estabelecimento da sessão PPPoE.

Só é possível se configurar endereços IP de interfaces de rede reconhecidas pelo sistema operacional no qual o firewall está rodando. Caso se tenha acrescentado uma nova interface de rede e seu nome não apareça na lista de interfaces, é necessário se configurar o sistema operacional de forma a reconhecer esta nova interface antes de tentar se configurá-la nesta pasta.

Rotas



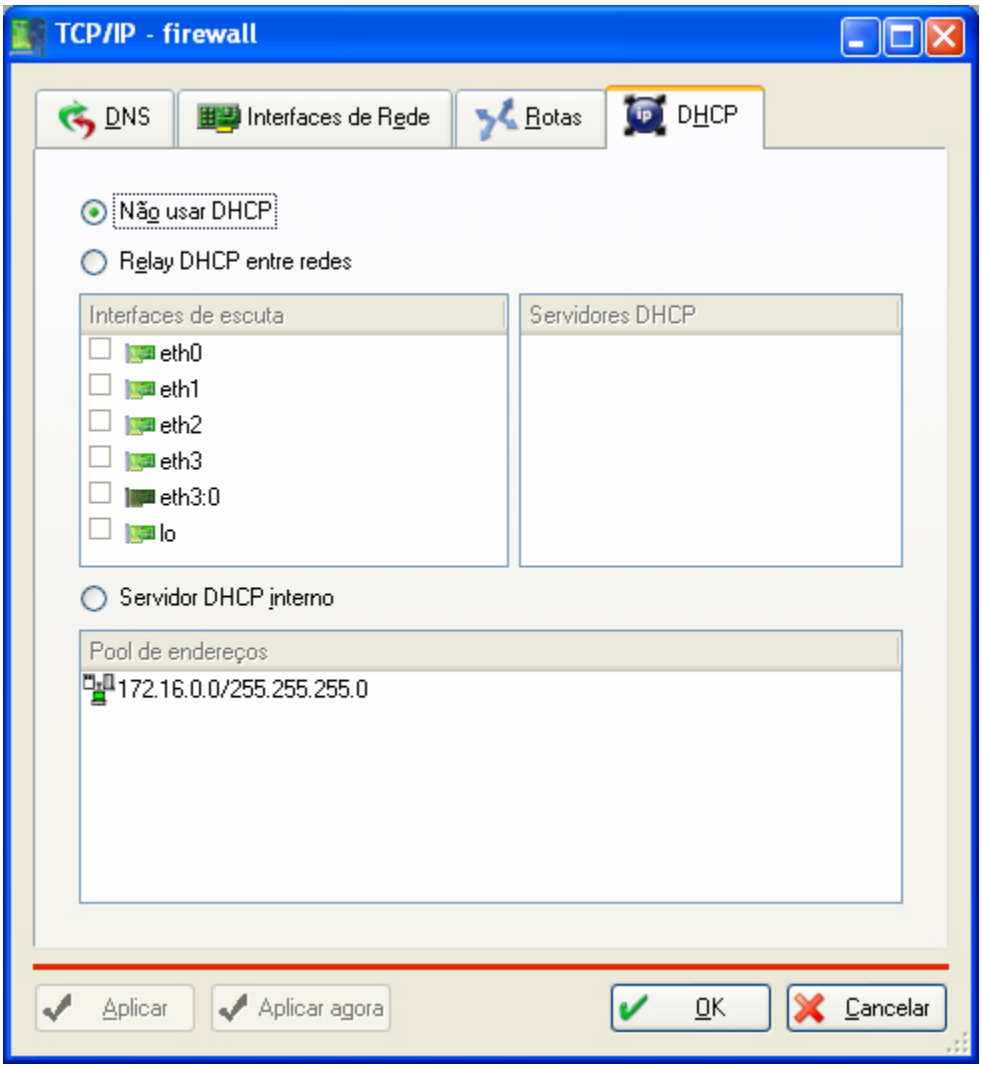
Esta pasta possibilita que se configure rotas IP no firewall. Ela consiste de um campo, chamado de **Rota Padrão**, onde se pode especificar o roteador padrão e de uma lista com as diversas rotas configuradas no firewall.

Para se incluir uma nova rota, basta se clicar no botão direiro do mouse e irá aparecer o menu 

.

Para se remover ou editar uma rota, basta se clicar com o botão direito sobre ela.

DHCP



Nesta pasta são definidas as opções do firewall em relação ao serviço DHCP. Ela consiste das seguintes opções:

Não usar DHCP: Se esta opção estiver selecionada o firewall não atuará como servidor DHCP nem efetuará relay entre redes conectadas a ele.

Relay DHCP entre redes: Esta opção permite que se defina que o firewall realizará o relay de pacotes DHCP entre as redes selecionadas. Ela é utilizada quando se possui apenas um servidor DHCP e se deseja que ele forneça endereços para máquinas localizadas em sub-redes distintas, conectadas diretamente ao firewall.

Ao se selecioná-la, deve-se especificar em **Interfaces de Escuta** as interfaces nas quais o firewall escutará broadcasts DHCP e os encaminhará para os servidores, especificados em **Servidores DHCP.** No caso de haver mais de um servidor, o firewall encaminhará as requisições para todos e retornará ao cliente a primeira resposta recebida.

Servidor DHCP Interno: Esta opção é designada para redes pequenas que não possuem um servidor DHCP ou que possuíam em um modem ADSL. Ela permite que o firewall atue como um servidor DHCP.

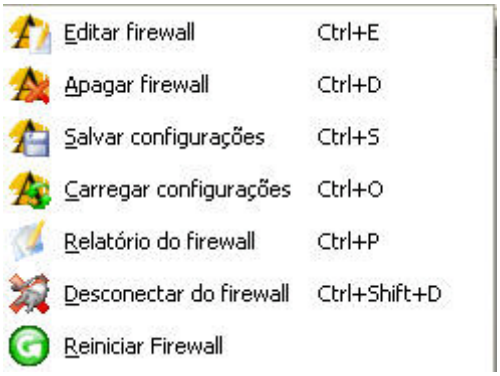
Ao se selecioná-la, deve-se especificar o pool de endereços, i.e. a faixa de endereços, que serão atribuídos aos clientes.

O firewall enviará aos clientes seu endereço como o servidor de DNS e seu domínio como nome do domínio para estes clientes.

29-10 Reinicializar Firewall

Esta opção serve para se reinicializar o firewall, porém não deve ser utilizada em condições normais de operação. A única operação que exige a reinicialização do firewall é a carga de um algoritmo de criptografia externo.

Para se reinicializar o firewall basta:

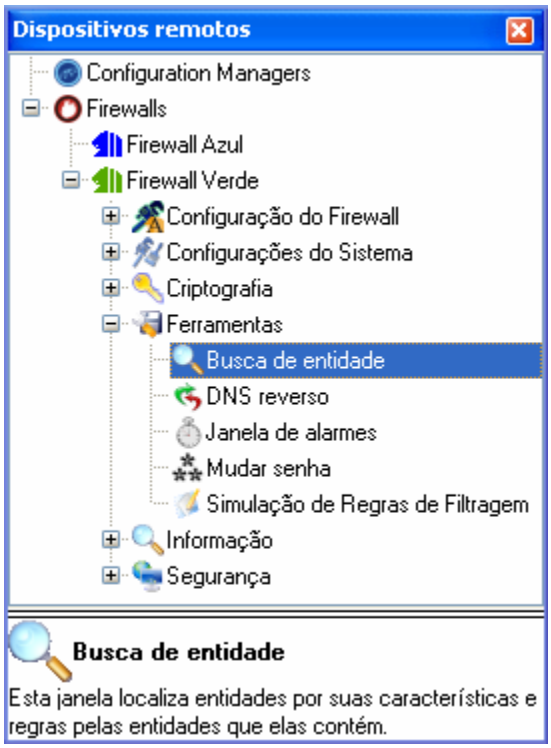


- Selecionar o firewall a ser reinicializado
- Selecionar o item *Reiniciar Firewall* no menu com o mesmo nome do firewall selecionado.

29-11 Busca Entidades

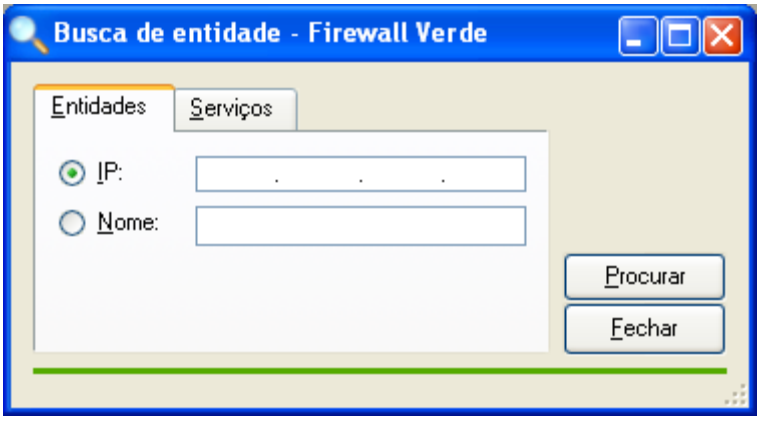
Esta opção permite que se localize entidades que contenham um determinado endereço IP, interface ou serviço, bem como regras que contenham uma determinada entidade.

Para se ter acesso à janela de localização de entidades basta:



- Clicar no menu *Ferramentas* da janela de administração do firewall
- Selecionar o item *Busca de entidade*

A janela de localização de entidades



Esta janela consiste de duas pastas onde cada uma é responsável por um tipo de pesquisa diferente:

- A pasta **Entidades** permite com que se localize entidades que contenham o endereço IP informado ou pelo seu nome.
- A pasta **Serviço** permite com que se localize entidades do tipo *serviço* que contenham o protocolo e o serviço especificados.

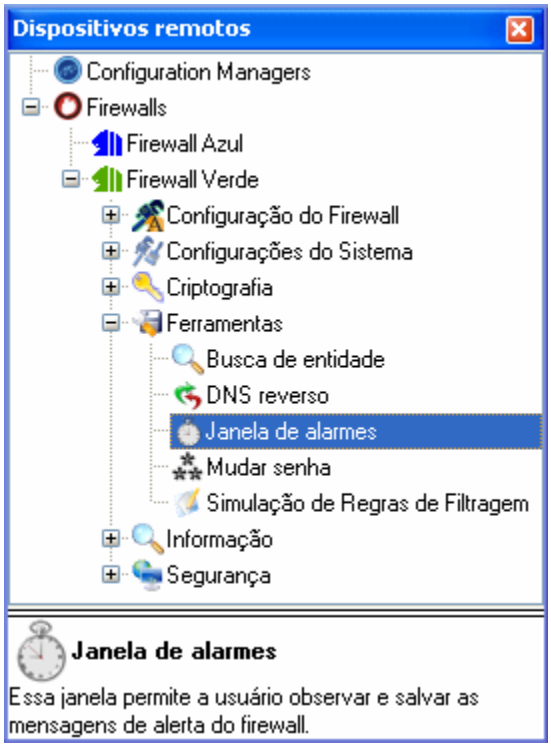
Independente da pesquisa utilizada, o funcionamento das janelas são idênticas:

- O botão **Procurar** inicia a busca a partir dos dados informados
- O botão **Fechar** fecha a janela de localização de entidades
- Ao se clicar duas vezes sobre o nome de uma entidade ou regra, mostrada como resultado da pesquisa, a janela de edição correspondente será aberta, possibilitando que se edite seus valores rapidamente.

29-12 Janela de Alarmes

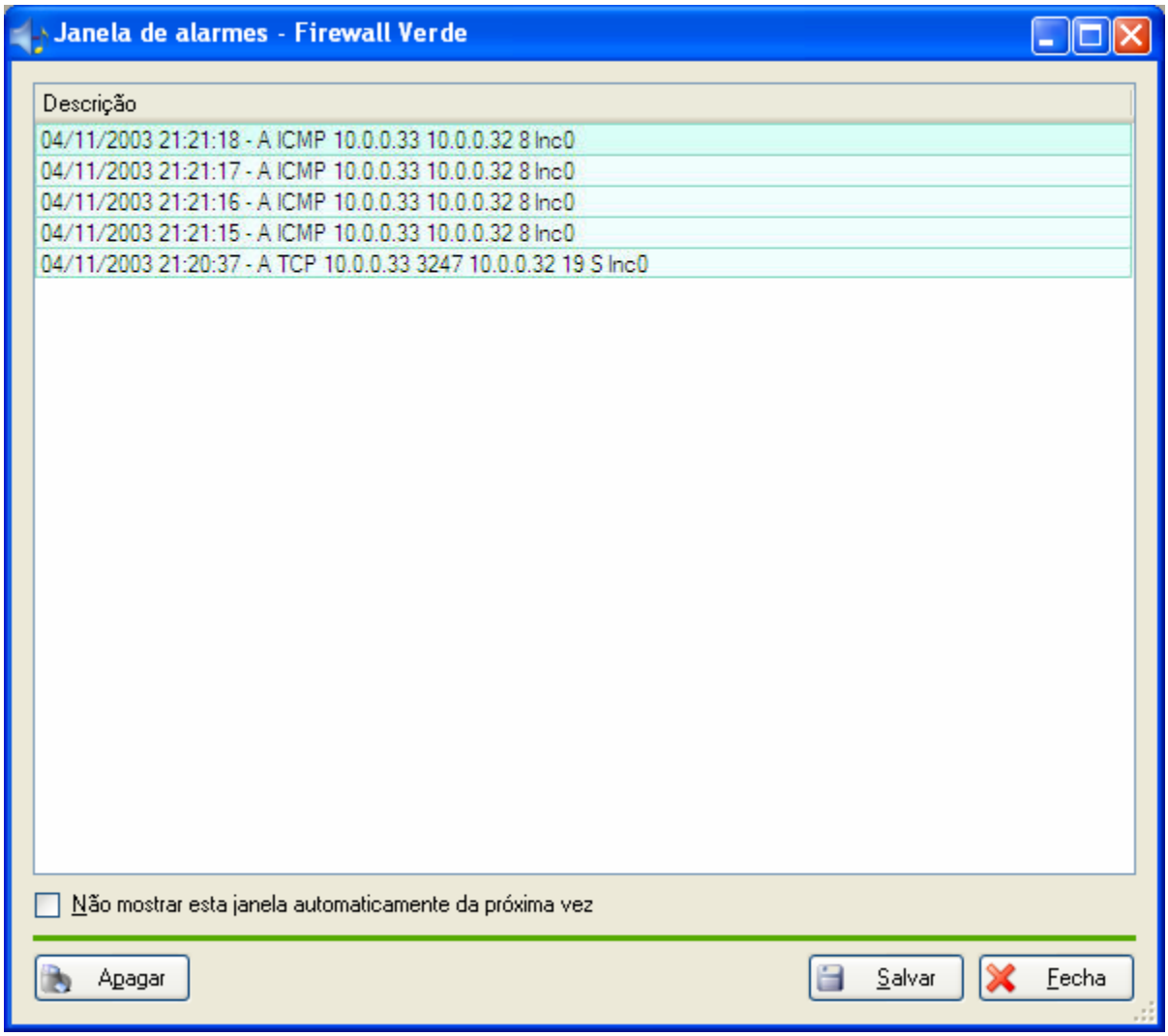
Esta opção permite que se visualize os alarmes gerados pelo firewall, quando esta opção estiver marcada nas regras de filtragem ou na janela de ações.

Para se ter acesso à janela de alarmes basta:



- Clicar no menu *Ferramentas* da janela de administração do firewall
- Selecionar o item *Janela de alarmes*

A janela de alarmes

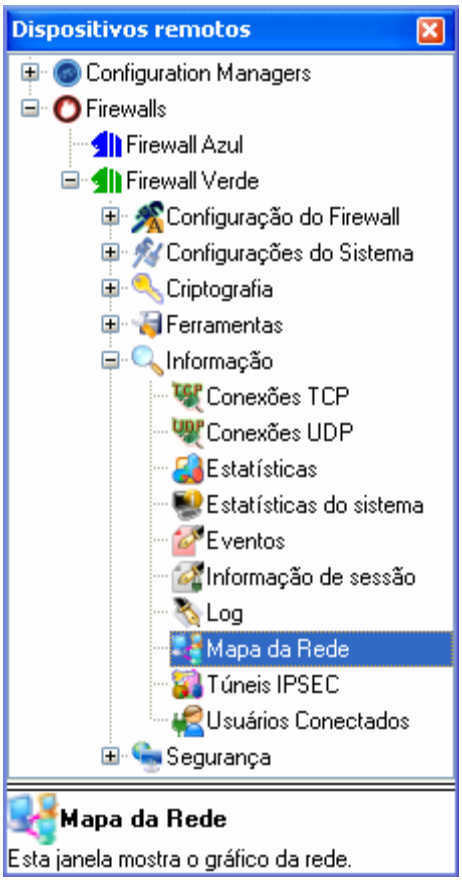


Esta janela consiste de um campo de descricao com as entradas correspondentes a acao executada pela regra de filtragem.

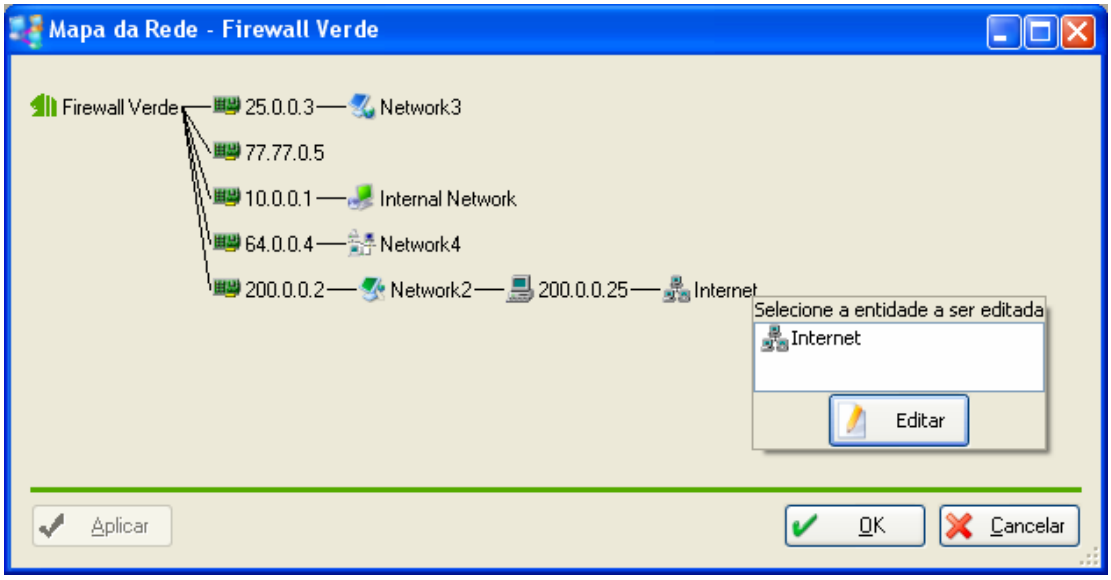
- O botão **Fechar** fará com que a janela seja fechada.
- A opção **Não mostrar essa janela automaticamente**, se estiver marcada, fará com que a janela nao seja mostrada automaticamente quando ocorrer um evento.
- O botão **Salvar** grava as entradas em um arquivo de log do tipo texto.
- O botão **Apagar** limpa todas as entradas contidas na janela.

29-13 Visualizando a rede graficamente

O firewall dispõe de um prático sistema para visualizar a rede onde ele se insere de forma gráfica. Para ter acesso à janela de visualização gráfica da rede, basta:



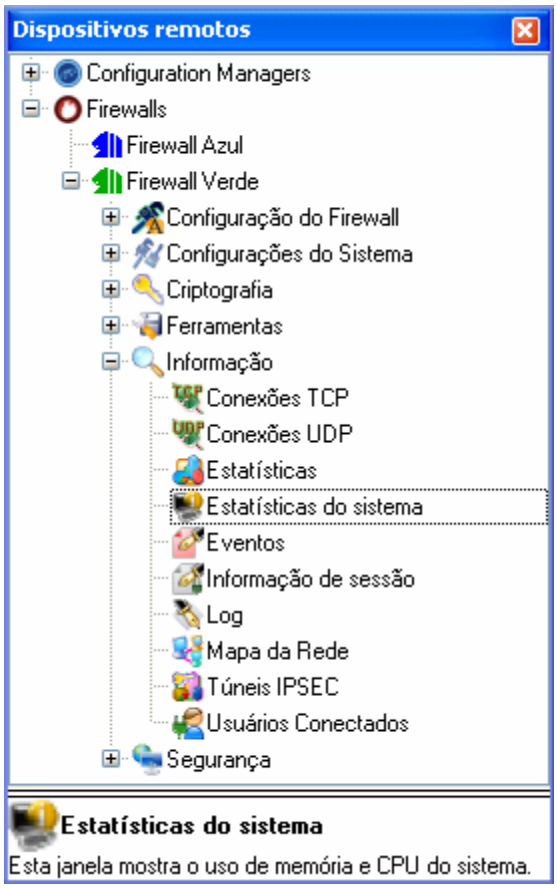
A janela a seguir aparecerá:



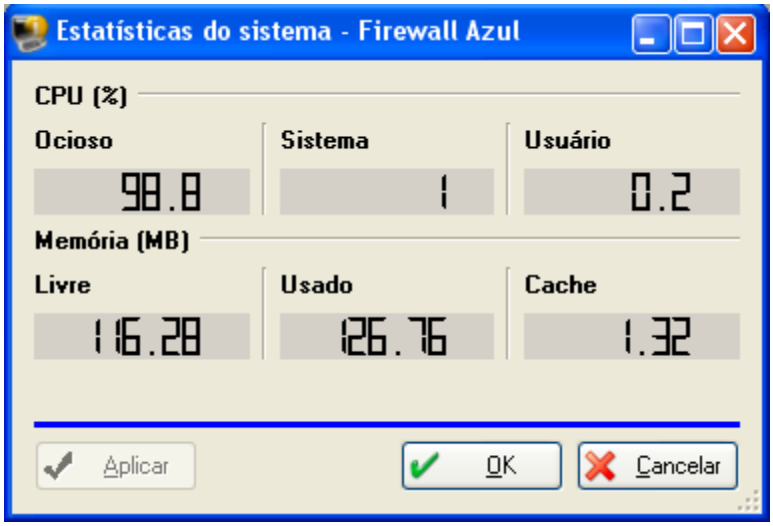
O primeiro ítem representa o firewall, conectado a suas interfaces de rede. A cada interface, se conectam uma ou mais redes e roteadores, que se conectam a mais redes distantes. Clicando em uma rede com o botão direito do mouse, aparecerá um menu listando as entidades que fazem parte da mesma, possibilitando ao usuário editá-las.

29-14 Visualizando estatísticas do sistema

A janela de estatísticas do sistema possui informações sobre uso do processador e uso de memória do sistema. Para ter acesso à essa janela, basta:



A janela a seguir aparecerá:



Na parte superior da janela são mostradas as informações de uso do CPU. Essas informações estão dividas em três partes: porcentagem ociosa, porcentagem dedicada ao sistema e porcentagem sendo usada por programas iniciados pelo usuário. A parte inferior da janela mostra a situação da memória do sistema em Megabytes. Também

está divida em três partes: quantidade de memória livre, quantidade de memória sendo usada e quantidade de memória armazenando informações em forma de cache.

A quantidade de memória não afeta de forma significativa a performance do firewall. Entretanto, pode ocorrer queda de desempenho se o sistema possuir área de memória swap e estiver fazendo muito uso dessa, o que irá afetar apenas os proxies.

É importante observar que a memória cache não é considerada memória usada. Ela é acessada apenas quando o sistema precisa reabrir um programa. Caso esse programa ainda esteja em cache, a reabertura será mais rápida. Porém, se o sistema precisar de uma quantidade maior de memória livre, a área usada para cache é liberada.

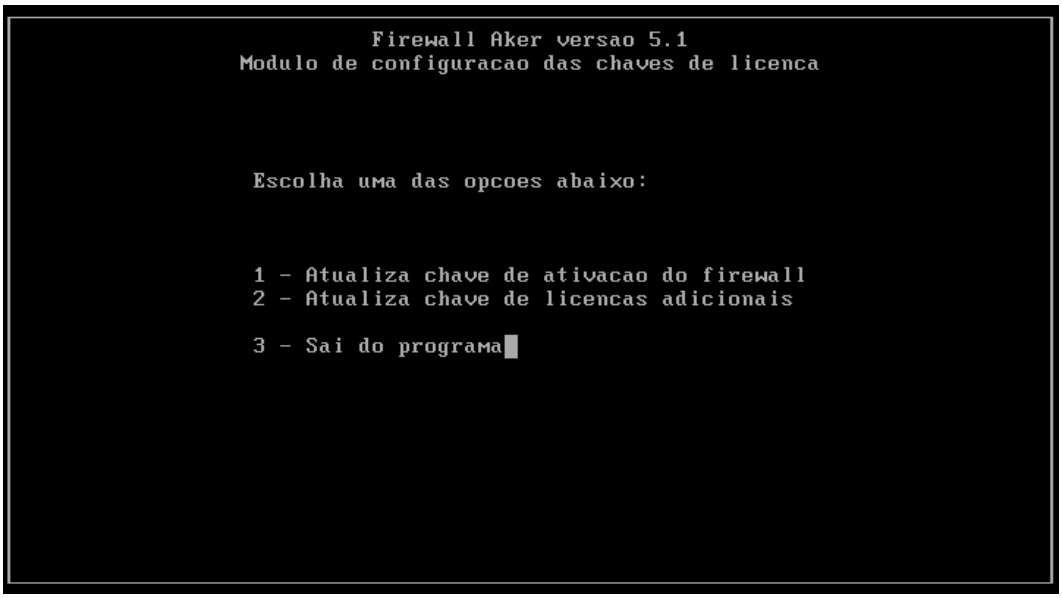
29-15 Utilizando a interface texto nas Chaves de Ativação

É possível configurar as Chaves de Ativação pela interface texto.

Localização do programa: `/etc/firewall/fwchave`

O programa é interativo e as opções de configuração são as descritas abaixo:

Escolhendo a opção será apresentado o mesmo programa de entrada de chave quando da instalação do firewall.


Firewall Aker versao 5.1
Modulo de configuracao das chaves de licenca
Escolha uma das opcoes abaixo:
1 - Atualiza chave de ativacao do firewall
2 - Atualiza chave de licencas adicionais
3 - Sai do programa

Digite os dados solicitados, conforme sua chave de ativação.

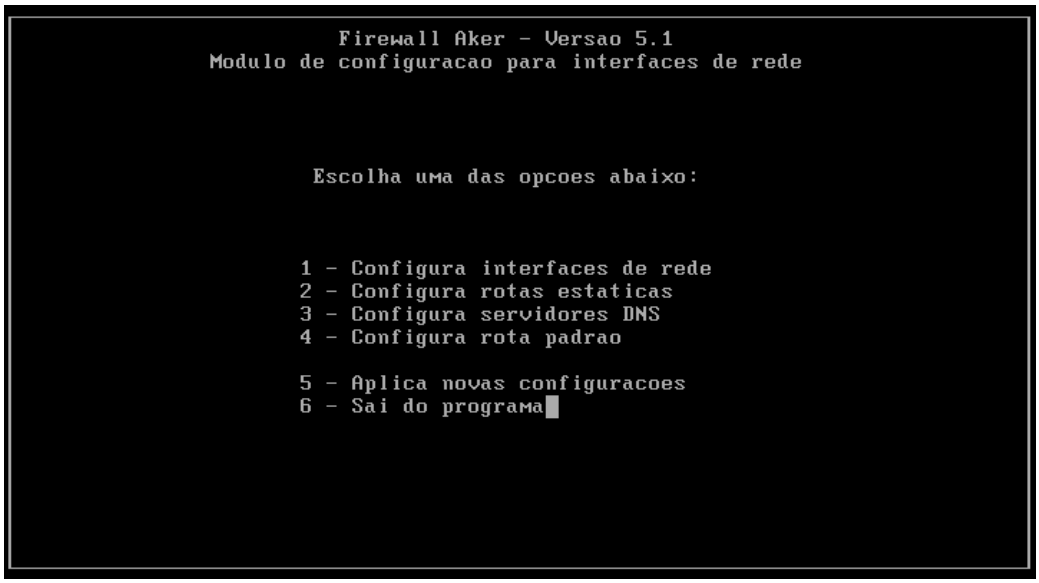
Firewall Aker versao 5.1
Modulo de configuracao das chaves de licenca
Configuracao da chave de ativacao
Nome da empresa: Aker Demo
IP da interface externa: 10.0.0.32
Chave de ativacao: A125545-5550055-44445222-5558AB555-55DDF555

29-16 Utilizando a interface texto na Configuração TCP/IP

É possível configurar os parâmetros do TCP/IP pela interface texto.

Localização do programa: `/etc/firewall/fwinterface`

O programa é interativo e as opções de configuração são as descritas abaixo:

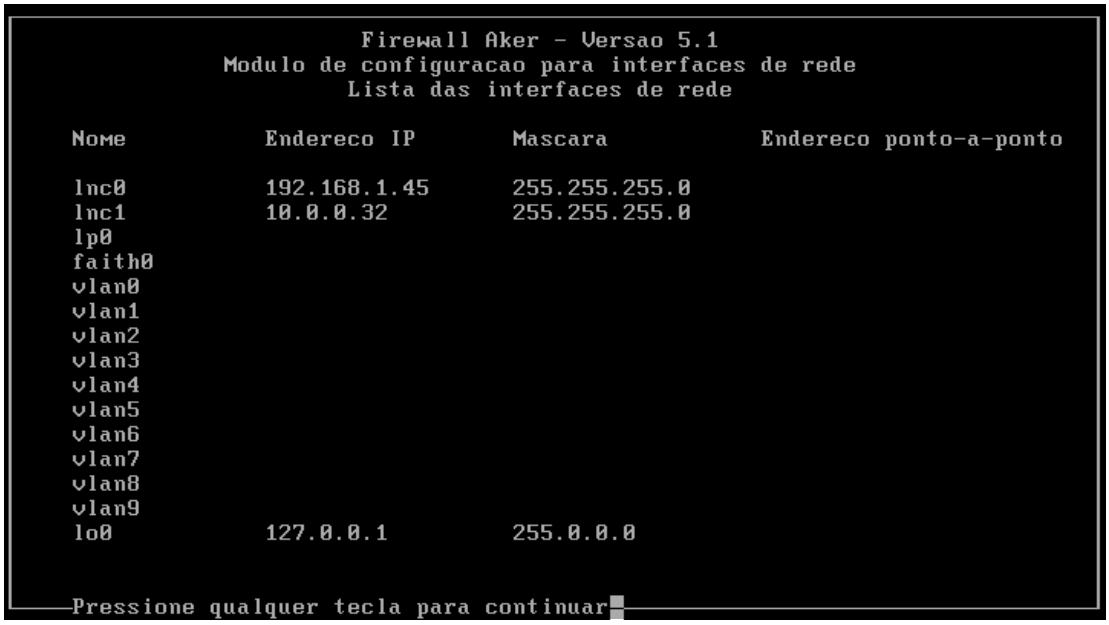

Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Escolha uma das opcoes abaixo:
1 - Configura interfaces de rede
2 - Configura rotas estaticas
3 - Configura servidores DNS
4 - Configura rota padrao
5 - Aplica novas configuracoes
6 - Sai do programa

Analogamente a configuração da interface gráfica, a interface texto possui 6 opções conforme visualizado na figura acima.

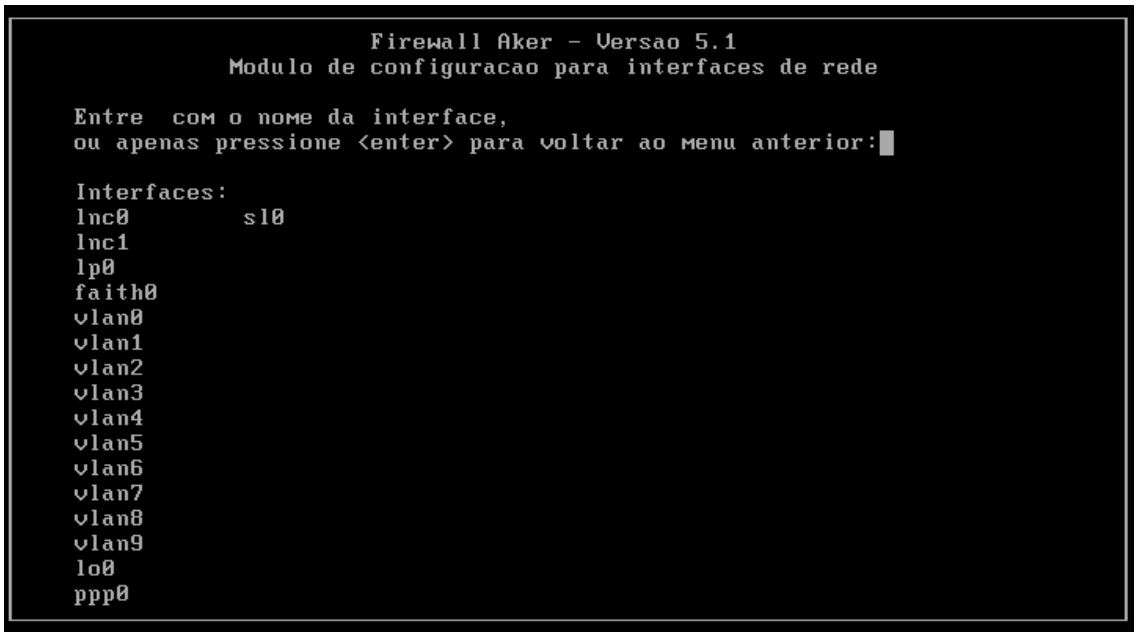
Na janela abaixo é possível visualizar, configurar e desconfigurar uma interface de rede

Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Configuracao de interfaces
1 - Listar interfaces
2 - Configurar interface
3 - Desconfigurar interface
4 - Sair

Na tela abaixo é apresentada a opção de listar interfaces



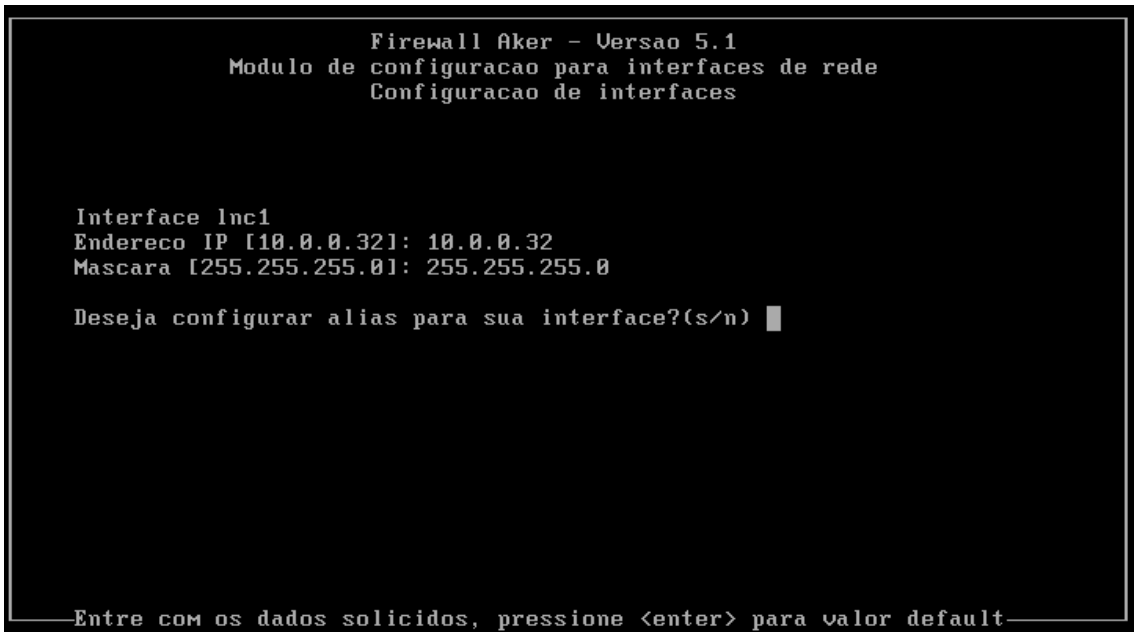
Para configurar uma interface basta digitar o nome da mesma. A tecla <enter> retorna ao menu anterior



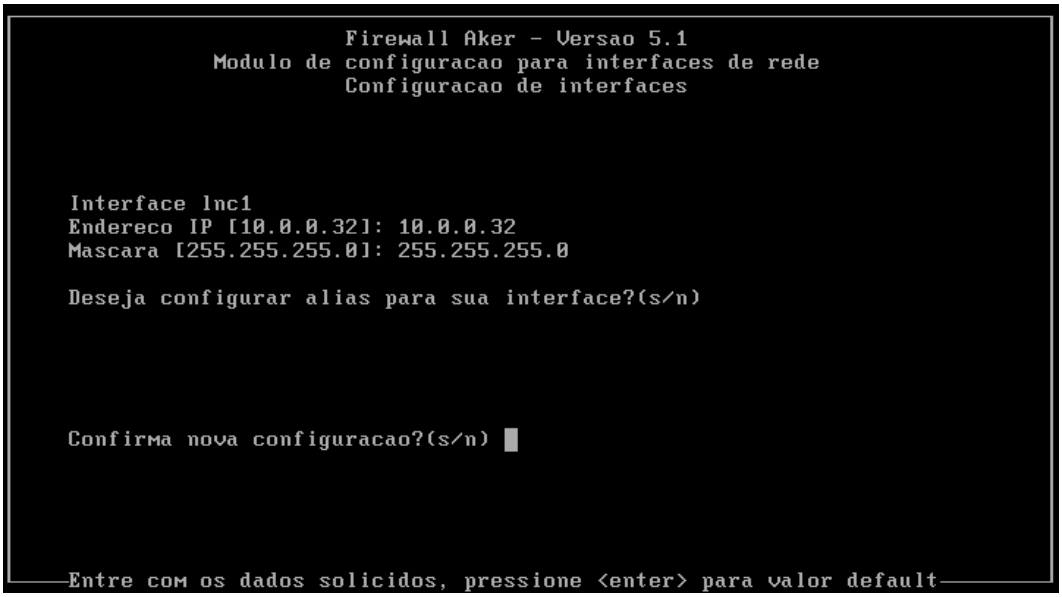
Nesta tela é apresentada a opção de se cadastrar VLAN

Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Configuracao de interfaces
Deseja configurar uma interface vlan filha para sua interface?(s/n)
Entre com os dados solicidos, pressione <enter> para valor default

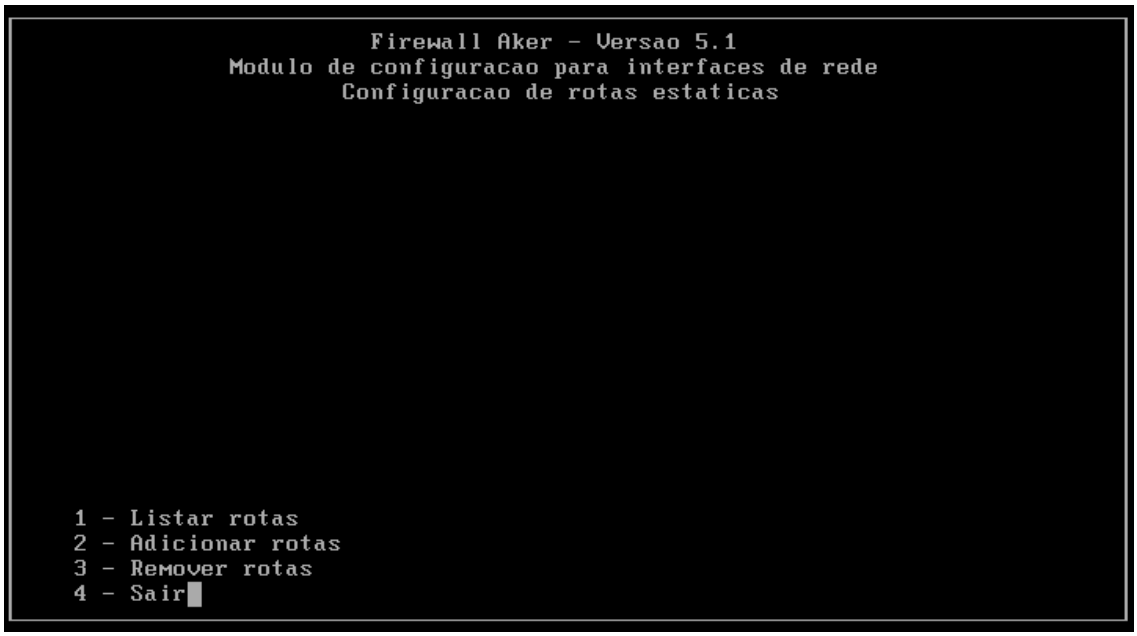
Após a digitação dos valores de configuração é perguntado se deseja configurar alias para a interface.


Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Configuracao de interfaces
Interface lnc1
Endereco IP [10.0.0.32]: 10.0.0.32
Mascara [255.255.255.0]: 255.255.255.0
Deseja configurar alias para sua interface?(s/n)
Entre com os dados solicidos, pressione <enter> para valor default

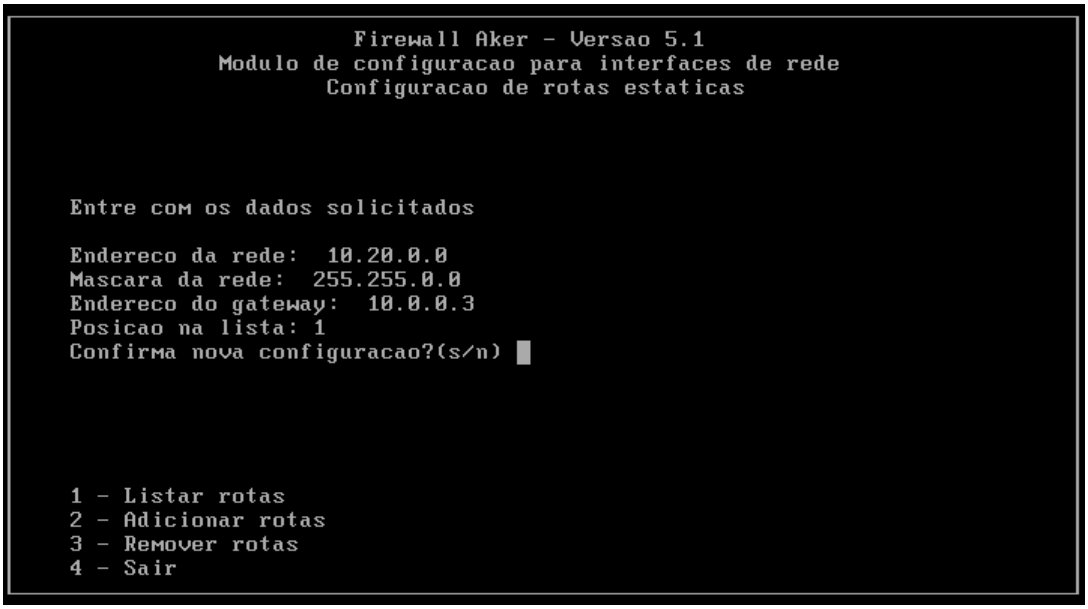
Com os dados já digitados é perguntado se deseja configurar interface para os novos valores.


Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Configuracao de interfaces
Interface lnc1
Endereco IP [10.0.0.32]: 10.0.0.32
Mascara [255.255.255.0]: 255.255.255.0
Deseja configurar alias para sua interface?(s/n)
Confirma nova configuracao?(s/n)
Entre com os dados solicidos, pressione <enter> para valor default

Após a digitação da Opção 2 da tela principal, é possível realizar a configuração de rotas estáticas.

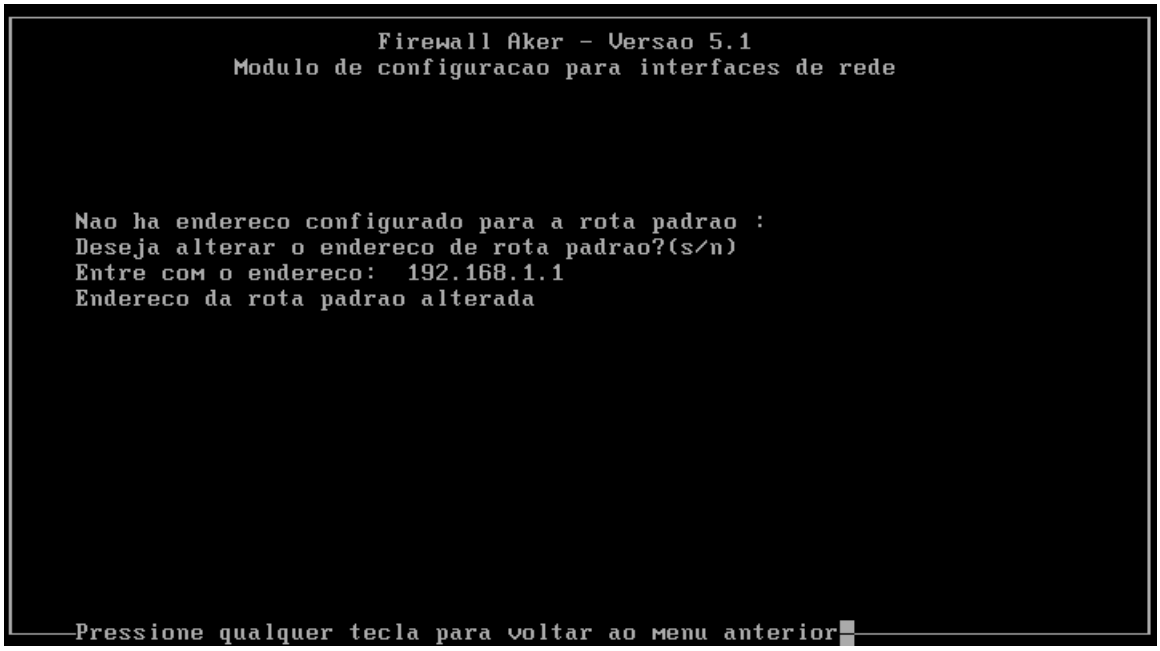

Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Configuracao de rotas estaticas
1 - Listar rotas
2 - Adicionar rotas
3 - Remover rotas
4 - Sair

Após as informações terem sido digitadas é perguntado se deseja gravar as novas configurações.

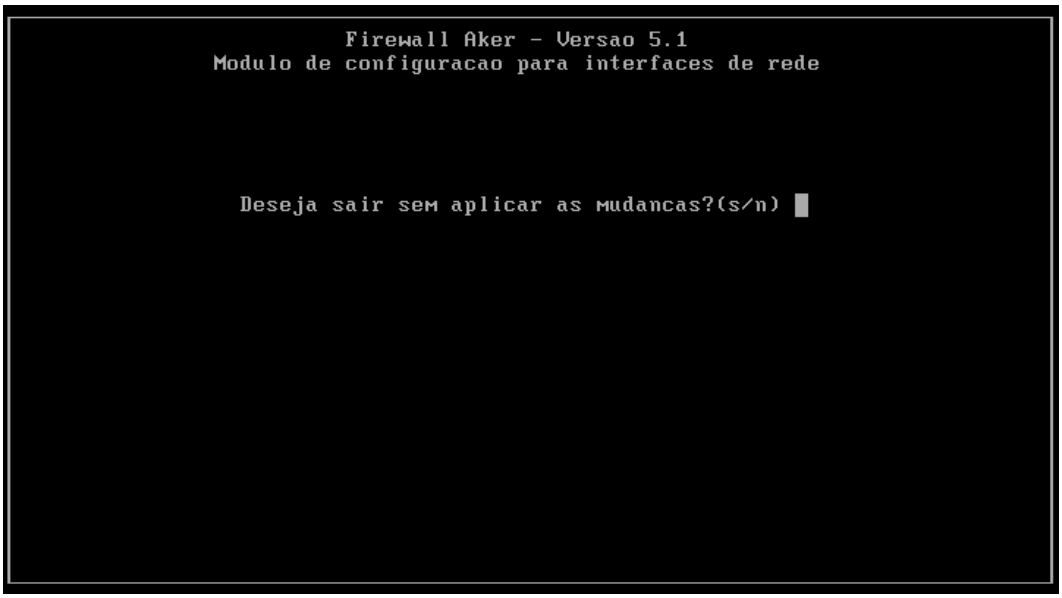

Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Configuracao de rotas estaticas
Entre com os dados solicitados
Endereco da rede: 10.20.0.0
Mascara da rede: 255.255.0.0
Endereco do gateway: 10.0.0.3
Posicao na lista: 1
Confirma nova configuracao?(s/n)
1 - Listar rotas
2 - Adicionar rotas
3 - Remover rotas
4 - Sair

Após a digitação da Opção 3 da tela principal, é possível realizar a configuração dos Servidores DNS.

Após a digitação da Opção 4 da tela principal, é possível realizar a configuração da rota padrão.


Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Nao ha endereco configurado para a rota padrao :
Deseja alterar o endereco de rota padrao?(s/n)
Entre com o endereco: 192.168.1.1
Endereco da rota padrao alterada
Pressione qualquer tecla para voltar ao menu anterior

A opção 5 permite aplicar as configurações realizadas. Caso o usuário escolha a opção 6 , qualquer modificação feita será detectada pelo firewall o qual perguntará se deseja sair sem aplicar as mudanças.


Firewall Aker - Versao 5.1
Modulo de configuracao para interfaces de rede
Deseja sair sem aplicar as mudancas?(s/n)

30-0 Configurando o Firewall em Cluster

Neste capítulo mostraremos como configurar a tolerância a falhas e o cluster cooperativo do Firewall Aker.

30-1 Planejando a Instalação

O que é um sistema de tolerância a falhas ?

Quanto mais os computadores ganham espaço nas empresas, nos escritórios e na vida das pessoas em geral, mais se houve falar em "alta disponibilidade". Por um simples e bom motivo: nenhum usuário quer que sua máquina pare de funcionar ou que os recursos de rede não possam mais ser acessados. É justamente a alta disponibilidade que vai garantir a continuidade de operação do sistema na prestação de serviços de rede, armazenamento ou processamento, mesmo se houver falhas em um ou mais de seus elementos.

Assim, alta disponibilidade é hoje um assunto que interessa a um número cada vez maior de usuários. E, sem dúvida, tornou-se um requisito fundamental para os sistemas que ficam no ar 24 horas por dia, sete dias por semana, ou que não possam ficar fora do ar por até mesmo alguns minutos. Afinal, paradas não planejadas podem comprometer, no mínimo, a qualidade do serviço, sem contar o prejuízo financeiro.

Tolerância a falhas nada mais é que um agrupamento de recursos que fornece ao sistema a ilusão de um recurso único. A maioria de seus componentes, senão sua totalidade, se encontra duplicado, desta forma, mesmo que um componente individual apresente falhas o serviço não é comprometido. Para possibilitar a redudância de recursos, é necessário um mecanismo de gerência de forma a tornar seu funcionamento transparente.

O que é um sistema Cooperativo?

No sistema de tolerância a falhas foi falado a respeito de alta disponibilitade e de agrupamento de recursos, mas no sistema cooperativo alem da alta disponibilidade ocorre o balanceamento de carga entre os sistemas. No sistema cooperativo todos os ficam ativos e se o peso entre eles for igual tratarão de forma balanceada as conexões e todos os processos entre eles.

Como trabalha a Tolerância a Falhas do Firewall Aker ?

A tolerância a falhas do Firewall Aker é composta por dois sistemas idênticos, ou seja, duas máquinas com o mesmo Sistema Operacional, mesmas placas de rede e com a mesma versão do Firewall, conectadas entre si. A exigência de se usar o mesmo sistema operacional se dá pelo fato de se poder aplicar correções através da interface gráfica e essas correções serem replicadas automaticamente de uma máquina para a outra.

Além de estarem conectadas entre si, o que deve ser feito por uma interface de rede, é necessário que todas as placas de rede correspondentes das duas máquinas estejam conectadas em um mesmo hub ou switch, de forma que ambos os firewalls tenham acesso às mesmas máquinas e roteadores.

Como trabalha o sistema Cooperativo do Firewall Aker ?

Antes de tudo a diferença básica da configuração do cluster cooperativo e do failover esta vinculada à licença. A licença do cluster cooperativo faz com que a convergência de dois firewalls com pesos iguais seja de 50% para cada um, já a licença do failover faz com que ocorra convergência em apenas um dos firewalls.

O que são modos UNICAST e MULTICAST do sistema Cooperativo do Firewall Aker ?

No Firewall Aker em modo cooperativo, mais de um host - os nodos do cluster - precisam receber os mesmos pacotes, para posteriormente cada um deles decidir se é de sua responsabilidade ou não. Como os switches não estão preparados nativamente para isso, uma de duas técnicas precisa ser empregada.

A primeira, chamada de modo unicast, implica em reconfigurar o switch para que ele saiba que um determinado endereço ethernet (MAC) está em duas ou mais portas simultaneamente, significando que ele deve copiar o pacote com esse endereço destino em todas elas, e jamais aprendê-lo como estando em uma porta apenas. Nesse modo, todos os firewalls do cluster usam o mesmo endereço MAC. O único incoveniente desse modo é que são raros os switches que o suportam.

A segunda, modo multicast, faz com que os firewalls de um cluster registrem um endereço ethernet multicast em suas interfaces e respondam as chamadas de ARP para o IP virtual com esse endereço. Se o switch não for configurado para limitar o espalhamento de pacotes multicast, todos os pacotes destinados ao firewall serão redistribuídos em todas as portas, como se fossem pacotes broadcast. Para fazer essa configuração, existem duas opções: ou se faz manualmente no switch, ou então se usa o protocolo IGMP, onde cada firewall anuncia ao switch que é membro do grupo multicast correspondente ao endereço escolhido. Seu switch deve suportar uma dessas duas opções. Além disso, existem alguns roteadores que não aprendem o endereço multicast ethernet da resposta ARP enviada pelo firewall. Nesses casos, as entradas para o firewall devem ser adicionadas manualmente em suas tabelas.

Existem implicações sérias de performance (flooding, por exemplo) e segurança (requisição de associação IGMP por qualquer host da rede) no caso de cluster no modo multicast. Todos os problemas podem ser evitados com corretas configurações nos switches. Tenha certeza que você entende o funcionamento desse modo antes de colocá-lo em funcionamento.

Quando o cluster estiver no ar, qualquer alteração feita nas configurações de um firewall através da interface gráfica será replicada automaticamente para o outro firewall.

30-2 Utilizando a interface texto

A utilização da interface texto na configuração da tolerância a falhas é bastante simples.

Localização do programa: `/etc/firewall/fwcluster`

Sintaxe:

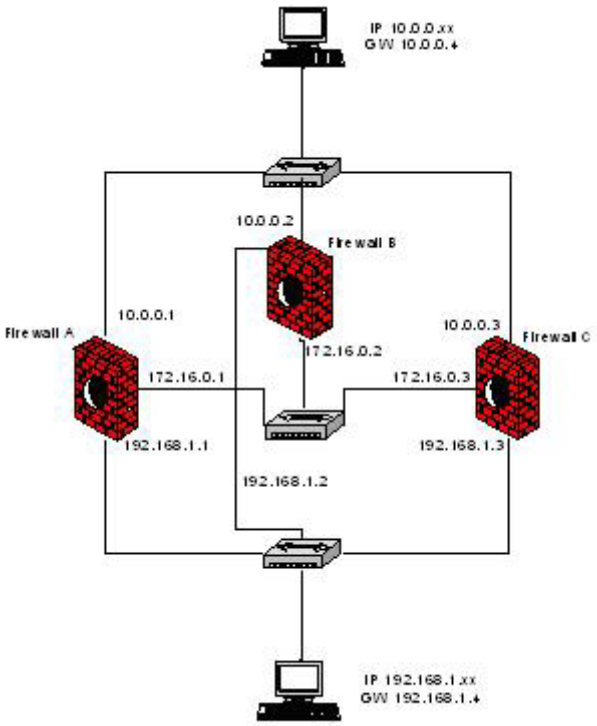
```
     fwcluster [ajuda | mostra]
     fwcluster interface_controle <if>
     fwcluster peso <peso>
     fwcluster <habilita | desabilita>
     fwcluster <inclui | remove> <if> [maquina | -f]
     fwcluster <modo> <if> [multicast [igmp <ip>] [mac <mac>] |
unicast]
```

Ajuda do programa:

```
Firewall Aker - Versao 5.1
Uso: fwcluster [ajuda | mostra]
     fwcluster interface_controle <if>
     fwcluster peso <peso>
     fwcluster <habilita | desabilita>
     fwcluster <inclui | remove> <if> [maquina | -f]
     fwcluster <modo> <if> [multicast [igmp <ip>] [mac <mac>] |
unicast]
(!) onde:
     if      : entidade interface
     peso    : peso deste firewall no cluster
     maquina : endereco IP virtual a remover ou incluir (entidade
maquina)
```

Exemplo 1: (mostrando a configuração)

Como efeito didático será explanada a topologia de uma rede com três firewalls em cluster e duas redes (rede 192 e rede 10).



Antes que se inicie a montagem do cluster, primeiramente devem ser cadastradas todas as interfaces, lembrando que diferente do cluster no firewall 4.5, aqui todos os firewalls possuem endereços ip diferentes.

Exemplos: Firewall A - rl0 - if_externa - 10.0.0.1 Firewall B - rl0 - if_externa - 10.0.0.2
rl1 - if_interna - 192.168.1.1 rl1 - if_interna - 192.168.1.2
rl2 - if_controle - 172.16.0.1 rl2 - if_controle - 172.16.0.2

Firewall C – rl0 - if_externa - 10.0.0.3
rl1 - if_interna - 192.168.1.3
rl2 - if_controle - 172.16.0.3

Em seguida crie uma entidade vitual para cada uma das placas, exeto para a interface de controle, essas entidades terão valor igual para todos os firewalls do cluster.

Exemplos: Firewall A - externa_firewall (ip 10.0.0.4) Firewall B - externa_firewall (ip 10.0.0.4)
interna_firewall (ip 192.168.1.4) interna_firewall (ip 192.168.1.4)

Firewall C - externa_firewall (ip 10.0.0.4)
interna_firewall (ip 192.168.1.4)

Para iniciar a configuração do cluster, crie primeiro a interface de controle:
/etc/firewall/fwcluster interface_controle interface_cadastrada

Depois inicie o cadastro de cada uma das interfaces participantes do firewall:
/etc/firewall/fwcluster inclui interface_cadastrada maquina_virtual_cadastrada

Defina o peso de cada Firewall, se não for definido, por padrão será aplicado peso 1 para todos:

/etc/firewall/fwcluster peso numero_do_peso

Após aplicar todas essas configurações em todos os firewalls participantes habilite o cluster em cada um deles:

/etc/firewall/fwcluster habilita

As máquinas do cluster não precisam ser iguais, mas as placas de rede sim.

Para o cluster failover utilize apenas 2 firewalls, já que apenas um responderá por todo o tráfego.

31-0 Arquivos do Sistema e Backup

Neste capítulo mostraremos onde estão localizados e para que são usados os arquivos que fazem parte da versão 5.0 do Firewall Aker.

31-1 Arquivos do Sistema

Neste tópico serão mostrados quais são e onde se localizam os arquivos do sistema. Isto é muito importante na hora de se realizar backups ou para se diagnosticar possíveis problemas de funcionamento.

Árvore de diretórios

- **`/etc/firewall`** - contém programas executáveis e sub-diretórios
- **`/etc/firewall/algs`** - contém os algoritmos de criptografia externos para o cliente de criptografia
- **`/etc/firewall/x509`** - contém os arquivos correspondenteas aos certificados X.509
- **`/etc/firewall/httpd`** - contém a raiz do sistema de arquivos do servidor local HTTP do proxy WWW. Não remova os arquivos já presentes neste diretório.
- **`/etc/firewall/conf`** - contém os arquivos de configuração do firewall
- **`/etc/firewall/snmpd`** - contém o agente SNMP
- **`/etc/firewall/root`** - não possui arquivos. É usado por alguns processos do Firewall
- **`/etc/firewall/run`** - contém arquivos necessários em tempo de execução
- **`/var/log`** - contém os arquivos de log e eventos do Firewall Aker
- **`/var/spool/firewall`** - usado pelos proxies SMTP e POP3 para armazenar as mensagens a serem enviadas
- **`/usr/src/sys/objs`** - contém os objetos pré-compilados do firewall usados para gerar um novo kernel para o sistema (apenas no FreeBSD)

Programas executáveis

Programas que podem ser executados pelos administradores do Firewall Aker

- **`/etc/firewall/fwadmin`** - Interface texto para administração de usuários
- **`/etc/firewall/fwaction`** - Interface texto para configuração das ações do sistema
- **`/etc/firewall/fwblink`** - Interface texto para configuração do balanceamento de links
- **`/etc/firewall/fwchave`** - Interface texto para configurar chave de ativação do sistema
- **`/etc/firewall/fwcert`** - Interface texto para configurar os certificados de criptografia
- **`/etc/firewall/fwclient`** - Interface texto para a configuração do acesso dos clientes de criptografia

- **/etc/firewall/fwcluster** - Interface texto para a configuração da tolerância a falhas
- **/etc/firewall/fwcripto** - Interface texto para configuração da criptografia e autenticação <>**/etc/firewall/fwedpwd** - Interface texto para configuração das bases de dados para autenticação local
- **/etc/firewall/fwent** - Interface texto para a criação de entidades
- **/etc/firewall/fwflood** - Interface texto para configuração da proteção contra SYN flood
- **/etc/firewall/fwids** - Interface texto para a configuração do suporte a agentes de detecção de intrusão
- **/etc/firewall/fwaccess -** Interface texto para a configuração das associações de perfis de acesso
- **/etc/firewall/fwlist -** Interface texto para acesso às conexões e sessões de usuários ativas
- **/etc/firewall/fwlog -** Interface texto para acesso ao log e aos eventos do firewall
- **/etc/firewall/fwmaxconn -** Interface texto para configuração do controle de flood
- **/etc/firewall/fwnat -** Interface texto para a configuração da conversão de endereços (NAT)
- **/etc/firewall/fwpar -** Interface texto para configuração dos parâmetros gerais
- **/etc/firewall/fwrule** - Interface texto para configuração do filtro de pacotes inteligente
- **/etc/firewall/fwupgrade** - Converte os arquivos de configuração da versão 3.52 , 4.0 ou 4.5 para a versão 5.0 do Firewall Aker.
- **/etc/firewall/fwipseccert** - Interface texto para a gerência os certificados X.509 necessários à criptofia IPSEC.
- **/etc/firewall/fwstat** - Interface texto para a configuração e visualização das estatísticas do Firewall.
- **/etc/firewall/fwinterface** - Interface texto para a configuração das interfaces de rede do Firewall.
- **/etc/firewall/fwauth** - Interface texto para a configuração dos parâmetros globais de autenticação do Firewall.

Programas que NÃO devem ser executados diretamente pelo administrador

- **/kernel** - Kernel modificado do sistema operacional com suporte ao Firewall Aker (apenas no FreeBSD)
- **/etc/firewall/aker_firewall_mod.ko** - Modulo carregável do kernel com o firewall (apenas no FreeBSD)
- **/etc/firewall/2.4.x/aker_firewall_mod-xxxx.o** - Modulo carregável do kernel com o firewall (apenas no Linux)
- **/etc/firewall/fwauthd** - Servidor de autenticação de usuários
- **/etc/firewall/fwcardd** - Modulo de validação de certificados X509 para smart cards
- **/etc/firewall/fwconfd** - Servidor de comunicação para a interface remota
- **/etc/firewall/fwcrld** - Módulo de download de CRLs das autoridades certificadoras ativas

- **/etc/firewall/fwcryptd** - Servidor de criptografia para clientes
- **/etc/firewall/fwdnsd** - Servidor de resolução de nomes (DNS) para a interface remota
- **/etc/firewall/fwidsd -** Programa de comunicação com agentes de detecção de intrusão
- **/etc/firewall/fwinit -** Programa de inicialização do Firewall Aker
- **/etc/firewall/fwftppd -** Proxy FTP transparente
- **/etc/firewall/fwgkeyd** - Servidor de geracao de chaves de criptografia
- **/etc/firewall/fwhttppd** - Proxy HTTP transparente e proxy WWW não transparente
- **/etc/firewall/fwheartd** - Serviço de controle do cluster
- **/etc/firewall/fwhconfd** - Serviço de configuração distribuída do cluster
- **/etc/firewall/fwgenericstd** - Serviço de coleta de informação distribuída do cluster
- **/etc/firewall/fwstconnd** - Serviçode replicação de conexões do cluster
- **/etc/firewall/fwlinkmond** - Serviço de monitoramento de links
- **/etc/firewall/fwdlavd** - Serviço de anti-vírus web
- **/etc/firewall/fwmachined** - Serviço de coleta de informações de performance
- **/etc/firewall/fwpmapd** - Proxy RPC transparente
- **/etc/firewall/fwlkeyd** - Servidor de certificados de criptografia
- **/etc/firewall/fwmond** - Módulo de monitoramento e reinicialização dos processos do firewall
- **/etc/firewall/fwnatmond** - Módulo de monitoramento de máquinas para o balanceamento de carga
- **/etc/firewall/fwprofd** - Servidor de login de usuários
- **/etc/firewall/fwrapd** - Proxy Real Player transparente
- **/etc/firewall/fwrtspd** - Real Time Streaming Protocol proxy
- **/etc/firewall/fwsocksd** - Proxy SOCKS não transparente
- **/etc/firewall/fwsmtppd** - Proxy SMTP transparente
- **/etc/firewall/fwpop3pd** - Proxy POP3 transparente
- **/etc/firewall/fwlogd -** Servidor de log, eventos e estatísticas
- **/etc/firewall/fwscanlogd -** Servidor de pesquisa de log, eventos e estatísticas
- **/etc/firewall/fwsyncd** - Processo de geração de sementes de criptografia e sincronia
- **/etc/firewall/fwtelnetd** - Proxy telnet transparente
- **/etc/firewall/fwtrap** - Módulo de envio de traps SNMP
- **/etc/firewall/fwurld** - Módulo de análise e checagem de permissão de acesso a URLs
- **/etc/firewall/fwiked** - Módulo de negociação de chaves para criptografia IPSEC (protocolo IKE)
- **/etc/firewall/fwtunneld** - Secure Roaming Server para Firewall
- **/etc/firewall/libaker.so** - Biblioteca genérica do firewall
- **/etc/firewall/libconfd.so** - Biblioteca de configuração do firewall
- **/etc/firewall/snmpd/snmpd** - Agente SNMP

Arquivos de Log, Eventos e Estatísticas

- **`/var/log/fw-510-AAAAMMDD.fwlg` -** Armazena os logs do firewall do dia DD/MM/YYYY
- **`/var/log/fw-510-AAAAMMDD.fwev` -** Armazena os eventos do firewall do dia DD/MM/YYYY
- **`/var/log/stat-510-AAAAMMDD.fws` -** Armazena as estatísticas do firewall do dia DD/MM/YYYY

31-2 Backup do Firewall

A versão 3.0 do Firewall Aker incorporou a possibilidade da realização de cópias de segurança e da recuperação completa de sua configuração remotamente. Isto foi demonstrado no capítulo intitulado Utilizando as ferramentas da interface gráfica. Este procedimento remoto é recomendado para a maioria das instalações, em virtude de sua facilidade de uso e da possibilidade da gravação de toda a configuração do firewall em uma máquina remota. Caso seja desejado, entretanto, é possível realizar a operação de backup manualmente, como feito na versão 2.0 e anteriores.

Neste tópico será mostrado o procedimento necessário para se realizar manualmente uma cópia de segurança completa (backup) do Firewall Aker e como recuperar uma instalação após um desastre.

Arquivos a serem copiados

- A parte mais importante a ser copiada são os arquivos de configuração apresentados no tópico anterior. Isto deve ser feito todas as vezes que se fizer alguma alteração na configuração do firewall.
- Outros arquivos importantes são os de log e eventos. Dependendo da necessidade de segurança, pode-se fazer cópias diárias ou até mais freqüentes destes arquivos. Uma outra opção para aumentar a segurança é configurar o Firewall para enviar o log e os eventos para o syslogd e configurar o syslogd para mandar estas mensagens para uma outra máquina da rede interna.

Para se realizar as cópias de segurança, pode-se utilizar o utilitário **`tar`** do FreeBSD e do Linux (os comandos abaixo devem ser executados pelo usuário root):

- **`tar cvfz /conf.tgz /etc/firewall/conf`**
  (salva toda a configuração do firewall no arquivo /`conf.tgz`)
- **`tar cvfz /log.tgz /var/log/*510*`**
  (salva os arquivos de log e de eventos no arquivo /`log.tgz`)

Após realizadas as cópias, pode-se transferir os arquivos `conf.tgz` e `log.tgz` para outras máquinas via, por exemplo, FTP.

Recuperação no caso de desastres

No caso de problemas que ocasionem a perda de dados, deve-se proceder da seguinte forma:

- Caso tenha-se perdido apenas os dados de configuração ou os arquivos de log e eventos, basta restaurar um dos backups citados acima.

É importante que nenhum processo do firewall esteja ativo no momento de restauração dos arquivos. Para se assegurar disso, pode-se reinicializar a máquina em modo mono-usuário ou matar todos os processos do firewall (isto pode ser feito através do comando **`kill `ps -ax | grep fw | grep -v grep | cut -c 1-5``**).
Para restaurar a cópia de segurança feita com o comando **`tar`** mostrado no tópico acima, deve-se executar a seguinte seqüência de comandos (os comandos devem ser executados pelo usuário root):

1. **`cd /`**
2. **`tar xvfz /conf.tgz`**
   (restaura os arquivos de configuração)
3. **`tar xvfz /log.tgz`**
   (restaura os arquivos de log)

- Caso tenha ocorrido uma perda generalizada, deve-se primeiro verificar se o sistema operacional se encontra intacto. Em caso de dúvida deve-se inicialmente reinstalar todo o FreeBSD ou Linux. Após isso, deve-se reinstalar o Firewall Aker, seguindo todos os procedimentos descritos no capítulo de instalação do sistema. Estando tudo funcionando, restaura-se os backups dos arquivos de configuração e de log e eventos, conforme mostrado acima.

32-0 Firewall Aker Box

Neste capítulo, mostraremos os comandos que podem ser utilizados no shell do Aker Firewall Box

O Firewall Aker Box

O Aker Firewall Box é composto por um sistema integrado de hardware e software. A grande vantagem dessa plataforma é que ela dispensa maiores conhecimentos de sistemas operacionais. Além disso, por não possuir disco rígido e por ser formada por um hardware industrial, a plataforma apresenta potencialmente maior resistência contra danos, especialmente picos de energia, o que acaba por possibilitar um funcionamento ainda mais estável.

O Firewall box está disponível em diversos modelos, que visam atender as necessidades de pequenas, médias e grandes empresas.

A lista completa dos modelos disponíveis é freqüentemente atualizada e está disponível em:

http://www.aker.com.br/index.php?pag_cod=8&prod_cod=21&ling=pt_br&cat_cod=8&itens=caracteristicas

Como funciona o shell do Aker Firewall Box?

Ao conectar-se um terminal serial comum configurado a 9600 bps à porta serial correspondente no Aker Firewall Box, será possível utilizar a interface de linha de comando do mesmo, isto é, seu shell.

Ao se realizar esse procedimento, primeiro será necessário apertar a tecla Enter até que apareça o pedido de senha, que inicialmente é '123456'. Entrando-se corretamente a senha, o prompt seguinte aparecerá:

```
Aker>
```

Caso se tenha perdido a senha de acesso local ao Firewall Aker Box, deve-se entrar em contato com o suporte técnico, para se realizar o procedimento de reset da mesma.

No prompt do shell, podem ser digitados todos os comandos normais do Firewall Aker, conforme documentados nos tópicos relativos à interface texto de cada capítulo. Além desses, existem comandos específicos ao firewall box que estão documentados abaixo.

É possível digitar os comandos do firewall no shell sem o prefixo fw, isto é, `ent` ao invés de `fwent`.

Para sair do shell, pode-se ou digitar os comandos `exit` ou `quit` ou simplesmente apertar as teclas Ctrl + D.

Comandos específicos do Aker Firewall Box

Comando	`quit` `exit`
Descrição	Encerram a sessão de administração no shell

Comando	`help` `?`
Descrição	Mostram uma tela com a lista de comandos válidos

Comando	`shutdown`
Descrição	Paralisa o firewall, para que ele possa ser desligado

Comando	`reboot`
Descrição	Reinicia o firewall

Comando	`ping [-c n_pkt] [-i interv] ip_destino`
Descrição	Envia pacotes ping para e espera a resposta do hosts `ip_destino` A opção `-c` especifica o número de pacotes a serem enviados A opção `-i` especifica o intervalo de transmissão entre os pacotes em milisegundos (ms)

Comando	`password`
Descrição	Troca a senha de acesso ao console do firewall

Comando	`date <mostra> | <dd/mm/aaaa>`
Descrição	Com o parâmetro `mostra`, informa a data do sistema. Senão, acerta a data para a informada.

Comando	`time <mostra> | <hh:mm[:ss]>`
Descrição	Com o parâmetro `mostra`, informa a hora do sistema. Senão, acerta o relógio para o horário informado.

Comando	`hd <-habilita | -desabilita>`
Descrição	Habilita ou desabilita o uso de um disco rígido

Apêndice A - Mensagens do sistema

Mensagens do log do Firewall

Todas as mensagens abaixo podem aparecer no log do firewall. Sempre que ocorrerem, elas estarão precedendo um registro que contém as informações sobre o pacote que as produziu. Na esquerda está sendo mostrado o número correspondente a cada uma das mensagens.

001 - Possível ataque de fragmentação

Esta mensagem indica que o filtro de pacotes recebeu um pacote TCP fragmentado no header TCP, possivelmente originado de uma tentativa de um ataque de fragmentação. Para maiores informações veja RFC 1858.

002 - Pacote IP direcionado

Esta mensagem indica que filtro de pacotes recebeu um pacote IP com uma das seguintes opções: Record Route, Loose Routing ou Strict Routing e ele foi configurado de modo a não aceitar pacotes IP direcionados. Para maiores informações veja RFC 791

003 - Ataque de land

Um ataque de land consiste em simular uma conexão de uma porta com ela mesma. Isto provoca o travamento da máquina atacada em boa parte das implementações TCP/IP.

Esta mensagem indica que o filtro de pacotes recebeu um pacote cujo endereço de origem é igual ao endereço destino e cuja porta de origem é igual à porta destino, caracterizando um ataque deste tipo.

004 - Conexão não consta na tabela dinâmica

Esta mensagem indica que o firewall recebeu um pacote TCP que não era de abertura de conexão e estava endereçado para uma conexão não aberta. Isto pode ser causado por um ataque ou simplesmente por uma conexão que ficou inativa por um tempo superior ao tempo limite para conexões TCP.

005 - Pacote proveniente de interface inválida

Esta mensagem indica que o filtro de pacotes recebeu um pacote IP proveniente de uma interface diferente da especificada na regra de filtragem na qual ele se encaixou. Isto pode ser causado por um ataque de falsificação de endereços IP (*IP spoofing*) ou por uma configuração errada de uma regra de filtragem.

006 - Pacote proveniente de interface não determinada

Esta mensagem indica que o filtro de pacotes recebeu um pacote mas não conseguiu determinar a interface de origem do mesmo. Como na regra de filtragem correspondente está especificada uma interface, o pacote foi rejeitado. Esta mensagem provavelmente nunca será mostrada.

007 - Conexão de controle não está aberta

Esta mensagem indica que o firewall recebeu um pacote de uma conexão de dados (de algum protocolo que utilize mais de uma conexão, como por exemplo o FTP e o Real Audio/Real Video) e a conexão de controle correspondente não estava aberta.

008 - Flags TCP do pacote são inválidos

Esta mensagem indica que o Firewall recebeu um pacote TCP cujos flags estavam inválidos ou contraditórios (por exemplo, SYN e FIN no mesmo pacote). Isto pode caracterizar um ataque ou uma implementação de TCP/IP defeituosa.

009 - Número de seqüência do pacote TCP inválido

Esta mensagem indica que o Firewall recebeu um pacote TCP cujo número de seqüência estava fora dos valores esperados. Isto pode caracterizar um ataque.

010 - Possível ataque de SYN Flood

Esta mensagem é gerada pelo Firewall todas as vezes que uma conexão é iniciada para um dos endereços protegidos contra SYN flood e a conexão não foi estabelecida dentro do prazo máximo estabelecido pelo administrador. Se esta mensagem ocorrer isoladamente, ou com pouca incidência, então provavelmente o intervalo de tempo configurado na proteção contra SYN flood (ver o capítulo de Proteção contra SYN Flood) está muito pequeno. Caso apareça um grande número destas mensagens seguidamente então provavelmente um ataque de SYN flood foi repelido pelo Firewall.

011 - Pacote sem informação de autenticação

Esta mensagem indica que pacote em questão veio sem header de autenticação e a configuração do fluxo seguro correspondente indica que ele só deveria ser aceito autenticado (ver o capítulo intitulado Criando Canais de Criptografia). Isto pode ser causado por uma configuração errada nos fluxos de autenticação (possivelmente só configurando em um dos lados da comunicação) ou por uma tentativa de ataque de falsificação de endereços IP (*IP spoofing*). Para maiores informações veja as RFCs 1825 e 1827.

012 - Pacote não passou pela autenticação

Esta mensagem indica que pacote em questão não foi validado com sucesso pelo módulo de autenticação do Firewall. Isto pode ser causado por uma configuração de chaves de autenticação inválida, por uma alteração indevida no conteúdo do pacote durante o seu trânsito ou por uma tentativa de ataque de falsificação de endereços IP (*IP spoofing*). Para maiores informações veja as RFCs 1825 e 1827.

013 - Pacote sem informação de criptografia

Esta mensagem indica que pacote em questão não veio criptografado e a configuração do fluxo seguro correspondente indica que ele deveria vir (ver o capítulo intitulado Criando Canais de Criptografia). Isto pode ser causado por uma configuração errada nos fluxos de criptografia (possivelmente só configurando em um dos lados da comunicação) ou por uma tentativa de ataque de falsificação de endereços IP (IP spoofing). Para maiores informações veja as RFCs 1825 e 1827.

014 - Tamanho do pacote a ser decriptado inválido

Esta mensagem indica que o módulo de criptografia detectou um tamanho do pacote a ser decriptado incompatível com o algoritmo de criptografia correspondente. Isto provavelmente é causado por uma configuração errada nos fluxos de criptografia.

015 - Decriptação do pacote apresentou erro

Esta mensagem indica que o módulo de criptografia, após decriptar o pacote e realizar os testes de consistência no mesmo, detectou que o mesmo é inválido. Isto provavelmente é causado por uma configuração errada da tabela de criptografia ou por um possível ataque de falsificação de endereços IP (*IP spoofing*).

016 - Tipo de encapsulamento do pacote inválido

Esta mensagem indica que o módulo de criptografia não reconheceu o tipo de encapsulamento usado neste pacote. Isto pode ser causado por uma falha na decriptação do pacote (devido a senhas erradas) ou por ter sido usado um tipo de encapsulamento não suportado. (O Firewall Aker trabalha exclusivamente com encapsulamento em modo de túnel, não aceitando outros modos, por exemplo, modo de transporte)

017 - Pacote sem informações de SKIP

Esta mensagem indica que pacote em questão não veio com um header SKIP e a configuração do fluxo seguro correspondente indica que ele deveria vir. Isto provavelmente é causado por uma configuração errada na tabela de criptografia onde um dos lados está configurado para usar SKIP ou Aker-CDP e o outro não (ver o capítulo intitulado Criando Canais de Criptografia).

018 - SA para o pacote não contém informações SKIP

Esta mensagem indica que o módulo de criptografia recebeu um pacote com um header SKIP e a associação de segurança (SA) correspondente não possui informações sobre SKIP (ver o capítulo intitulado Criando Canais de Criptografia). Isto provavelmente é causado por uma configuração errada na tabela de criptografia onde possivelmente um dos lados está configurado para usar SKIP ou Aker-CDP e o outro não.

019 - Versão do protocolo SKIP inválida

Esta mensagem indica que a versão do protocolo SKIP indicada no pacote em questão é diferente da versão suportada. (O Firewall Aker implementa a versão 1 do protocolo SKIP)

020 - Valor do contador do protocolo SKIP inválido

O protocolo SKIP envia em cada pacote um contador, que é incrementado de hora em hora, com o objetivo de evitar ataques de repetição de seqüência. Esta mensagem indica que o contador recebido no pacote em questão é inválido. Isto pode ter duas causas distintas: ou relógio interno dos dois firewalls se comunicando está defasado em mais de uma hora ou ocorreu uma tentativa de ataque de repetição de seqüência.

021 - SPI inválido para autenticação com SKIP

Esta mensagem indica que foi recebido um pacote SKIP cujo número de SPI especificado no cabeçalho de autenticação era inválido. (O protocolo SKIP exige que o número do SPI utilizado seja 1)

022 - Próximo protocolo do cabeçalho SKIP inválido

Esta mensagem indica que o protocolo seguinte ao cabeçalho SKIP do pacote em questão não é suportado. (O Firewall Aker exige que após o cabeçalho SKIP venha o cabeçalho de autenticação)

023 - Algoritmo de autenticação do SKIP inválido

Esta mensagem indica que o algoritmo de autenticação especificado no cabeçalho SKIP não é suportado (O Firewall Aker somente suporta os algoritmos de autenticação MD5 e SHA-1).

024 - Algoritmo de criptografia do SKIP inválido

Esta mensagem indica que o algoritmo de criptografia especificado no cabeçalho SKIP não é suportado. (O Firewall Aker somente suporta os algoritmos de criptografia DES, Triplo DES e Blowfish, com 128 e 256 bits de chaves)

025 - Algoritmo de criptografia de chave SKIP inválido

Esta mensagem indica que o algoritmo de criptografia e separação de chaves especificado no cabeçalho SKIP não é suportado. (O Firewall Aker somente suporta os algoritmos DES, com MD5 como separador de chaves, Triplo DES, com MD5 como separador de chaves e Blowfish, com MD5 como separador de chaves)

026 - Algoritmo de compressão de dados não suportado

Esta mensagem indica que o algoritmo de compressão de dados especificado no cabeçalho SKIP não é suportado. (O Firewall Aker não suporta nenhum algoritmo de compressão de dados, uma vez que estes ainda não estão padronizados)

027 - Identificador de espaço de nome de origem inválido

O protocolo SKIP permite que sejam utilizados outros espaços de nomes, que não endereços IP, para selecionar a associação de segurança correspondente (SA). O espaço de nome pode ser especificado para a origem e/ou para o destino. Esta mensagem indica que o espaço de nome de origem não é suportado. (O Firewall Aker somente suporta endereços IP como espaço de nome)

028 - Identificador de espaço de nome de destino inválido

O protocolo SKIP permite que sejam utilizados outros espaços de nomes, que não endereços IP, para selecionar a associação de segurança correspondente (SA). O espaço de nome pode ser especificado para a origem e/ou para o destino. Esta mensagem indica que o espaço de nome de destino não é suportado. (O Firewall Aker somente suporta endereços IP como espaço de nome)

029 - Versão do protocolo Aker-CDP inválida

Esta mensagem indica que o Firewall recebeu um pacote do protocolo Aker-CDP com versão inválida.

030 - Tamanho do pacote para protocolo Aker-CDP inválido

Esta mensagem indica que o Firewall recebeu um pacote do protocolo Aker-CDP com tamanho inválido.

031 - Autenticação de pacote de controle Aker-CDP inválida

Esta mensagem indica que o Firewall recebeu um pacote de controle do protocolo Aker-CDP com autenticação inválida. As causas prováveis são uma modificação do pacote durante o trânsito ou uma possível tentativa de ataque.

032 - Número de licenças do firewall atingido

O Firewall Aker é vendido em diferentes faixas de licenças, de acordo com o número de máquinas da(s) rede(s) interna(s) a serem protegidas. Esta mensagem indica que o firewall detectou um número de máquinas internas maior que o número de licenças adquiridas e devido a isso impediu que as máquinas excedentes abrissem conexões através dele.

Solução: Contate a Aker Security Solutions ou seu representante autorizado e solicite a aquisição de um maior número de licenças.

033 - Pacote descartado por uma regra de bloqueio IDS

Esta mensagem indica que o Firewall recebeu um pacote que se enquadrou em uma uma regra temporária acrescentada pelo agente de detecção de intrusão e, devido a isso, foi descartado (para maiores informações veja o capítulo intitulado Configurando o Agente de Detecção de Intrusão).

034 - Header AH com formato incorreto (campo: length)

Esta mensagem indica que o Firewall recebeu um pacote cifrado com criptografia IPSEC que tem informações de autenticação no protocolo AH com tamanho incorreto. Veja a RFC 2402.

035 - Tunelamento AH e ESP simultâneos não permitido

Esta mensagem indica que o Firewall recebeu um pacote cifrado com criptografia IPSEC duplamente tunelado (via ESP e AH). Isto não é permitido.

036 - SA para este pacote não foi negociada

Esta mensagem indica que o Firewall recebeu um pacote cifrado com criptografia IPSEC para um canal não negociado.

037 - Padding exigido muito grande

Esta mensagem indica que o Firewall calculou um tamanho de preenchimento para o protocolo ESP maior que o permitido. Provavelmente o tamanho de bloco do algoritmo de criptografia é demasiado grande.

038 - Tamanho de padding decifrado incorreto

Esta mensagem indica que o firewall decifrou um pacote que dizia ser maior do que efetivamente é, via criptografia IPSEC. Provavelmente o pacote está corrompido ou houve erros na troca de chaves.

039 - Erro iniciando autenticação para o algoritmo especificado

Esta mensagem indica que o Firewall não conseguiu autenticar o pacote com o algoritmo HMAC. Provavelmente o algoritmo de autenticação está com defeito.

040 - Erro finalizando autenticação com o algoritmo escolhido

Esta mensagem indica que o Firewall não conseguiu autenticar o pacote com o algoritmo HMAC. Provavelmente o algoritmo de autenticação está com defeito.

041 - Final de conexão

Esta mensagem é apenas um registro de final de conexão e não deve aparecer normalmente no log do firewall.

042 - Limite configurado de conexões a partir do endereço IP excedido

Esta mensagem ocorre quando o limite máximo de conexões configurado pelo modulo proteção contra flood tiver sido atingido. Para verificar a configuração deste módulo consulte a Proteção de Flood.

Mensagens dos eventos do Firewall

043 - Firewall Aker v5.0 - Inicialização completa

Esta mensagem tem caráter puramente informativo, servindo para se determinar os horários que o Firewall entrou em funcionamento. Ela será produzida a cada reinicialização da máquina.

044 - Erro de alocação de memória

Esta mensagem indica que algum módulo do Firewall tentou alocar memória e não conseguiu. Esta mensagem pode ocorrer em sistemas com pouca memória RAM utilizando conversão de endereços com um grande número de conexões simultâneas ou com um grande número de conexões ativas passando pelos proxies do firewall.

Solução: Adquira mais memória RAM ou aumente as partições de swap.

045 - Tabela de conversão TCP cheia

A tabela de conversão de endereços TCP encheu. A única solução para esse problema é diminuir o Tempo limite TCP nos parâmetros de configuração. Para maiores informações veja o capítulo Configurando os parâmetros do sistema.

046 - Tabela de conversão UDP cheia

A tabela de conversão de endereços UDP encheu. A única solução para esse problema é diminuir o Tempo limite UDP nos parâmetros de configuração. Para maiores informações veja o capítulo Configurando os parâmetros do sistema.

047 - Tabela de criptografia para clientes cheia

Esta mensagem indica que um cliente de criptografia tentou estabelecer uma sessão de criptografia com o firewall, entretanto, o número sessões estabelecidas já atingiu o limite configurado no sistema.

Solução: Aumente o valor do número máximo de sessões simultâneas para clientes de criptografia. Se necessário, contate a Aker Consultoria e Informática ou seu representante autorizado e solicite a aquisição de um maior número de licenças de clientes de criptografia.

048 - Algoritmo de autenticação inválido

O módulo de criptografia detectou um algoritmo de autenticação inválido na associação de segurança quando realizava a criptografia de um pacote.

Solução: Contate o suporte técnico

049 - Algoritmo de criptografia inválido

O módulo de criptografia detectou um algoritmo de criptografia inválido na associação de segurança quando realizava a criptografia de um pacote.

Solução: Contate o suporte técnico

050 - Dados inválidos recebidos pela carga do Firewall

Esta mensagem indica que foram enviados dados inválidos para os módulos do Firewall que rodam dentro do kernel do FreeBSD ou Linux. Os dados inválidos devem necessariamente ter sido produzidos por um programa rodando na máquina do firewall.

Solução: Procure verificar qual programa produz esta mensagem ao ser executado e não execute-o mais.

051 - Erro ao ler o arquivo de parâmetros

Esta mensagem é produzida por qualquer um dos módulos externos ao tentar ler o arquivo de parâmetros do sistema e constatar que este não existe ou não pode ser lido.

Solução: Reinicialize a máquina, que o programa de inicialização irá recriar o arquivo de parâmetros. Se isso não funcionar, contate o suporte técnico.

052 - Erro ao carregar perfis de acesso

Esta mensagem indica que o servidor de autenticação ou o servidor de login de usuários não conseguiu carregar a lista de perfis de acesso cadastrados no sistema.

Solução: Contate o suporte técnico.

053 - Erro ao carregar entidades

Esta mensagem indica que algum processo servidor do firewall não conseguiu carregar a lista de entidades cadastradas no sistema.

Solução: Contate o suporte técnico.

054 - Nome de perfil de acesso inválido

Esta mensagem indica que o servidor de autenticação ao procurar o perfil de acesso de um usuário constatou que o mesmo não se encontra cadastrado no sistema.

Solução: Contate o suporte técnico.

055 - Erro ao criar socket de conexão

Esta mensagem indica que algum dos módulos externos tentou criar um socket e não conseguiu.

Solução: Verifique o número de arquivos que podem ser abertos por um processo e o número total para o sistema. Se necessário aumente estes valores. Para maiores informações de como fazer isso, contate o suporte técnico.

056 - Tamanho da linha excessivo

Esta mensagem indica que algum proxy do Firewall Aker recebeu uma linha com um número excessivo de caracteres e devido a isso, derrubou a conexão. A informação complementar entre parênteses indica o endereço IP da máquina que causou o problema.

Solução: Esta mensagem é causada por um servidor ou cliente fora dos padrões das RFCs. A única solução possível para o problema é contatar o administrador da máquina causadora da mensagem.

057 - Erro ao carregar contexto

Esta mensagem indica que um dos proxies transparentes não conseguiu carregar o contexto especificado.

Solução: Contate o suporte técnico.

058 - Erro ao carregar tabela de criptografia

Esta mensagem indica que um dos servidores do firewall não conseguiu carregar a tabela de criptografia.

Solução: Contate o suporte técnico.

059 - DNS reverso não configurado

Esta mensagem é produzida por algum dos proxies se ele tiver sido configurado para somente receber conexões a partir de máquinas com DNS reverso válido e não tiver conseguido resolver o nome para o endereço IP de origem de uma conexão. A mensagem complementar indica o endereço IP de origem da conexão.

060 - DNS direto e reverso conflitantes

Quando um proxy do Firewall é configurado para somente aceitar conexões a partir de máquinas com DNS reverso válido, ele utiliza uma técnica que consiste em tentar resolver o nome para o endereço IP de origem da conexão. Caso ele não consiga, ele indica erro mostrando a mensagem anterior e não permite a realização da conexão. Caso resolva o nome, ele faz uma outra pesquisa de DNS a partir do nome retornado, buscando seu endereço IP. Se ele não conseguir realizar esta segunda pesquisa ou se o endereço IP retornado for diferente do endereço de origem, a conexão é abortada e esta mensagem é produzida.

061 - Possível ataque de simulação de protocolo

Esta mensagem indica que o firewall durante o monitoramento de uma sessão de algum protocolo com várias conexões (por exemplo, FTP e Real Audio / Real Video) detectou uma tentativa de abertura de conexão para uma porta menor que 1024 ou para um endereço diferente do esperado. Isso provavelmente é causado por um ataque ou por uma implementação defeituosa do protocolo.

A mensagem complementar indica os endereço de origem e destino da conexão.

062 - Comando inválido

Esta mensagem indica que um dos proxies recebeu um comando considerado inválido da máquina cliente e devido a isso não repassou-o para o servidor. As mensagens complementares indicam qual o comando que tentou ser executado e quais as máquinas de origem e destino (no caso de proxy transparente) da conexão.

063 - Mensagem SMTP aceita

Esta mensagem indica que o proxy SMTP transparente aceitou uma mensagem e a enviou para o servidor. A mensagem complementar indica quais as máquinas de origem e destino da conexão e quem são o remetente e o destinatário da mensagem.

064 - Mensagem SMTP rejeitada

Esta mensagem indica que o proxy SMTP transparente rejeitou uma mensagem recebida. Isto foi causado por a mensagem ter se encaixado em algum filtro que indicava que ela deveria ser rejeitada ou por ter um tamanho maior que o tamanho máximo permitido.

065 - Conexão SMTP bloqueada por regra de DNS

Esta mensagem indica que o proxy SMTP bloqueou uma conexão devido a uma regra da para de DNS. Para mais informações leia o capitulo intitulado Configurando o proxy SMTP .

066 - Conexão SMTP bloqueada por RBL

Esta mensagem indica que o proxy SMTP bloqueou uma conexão devido ao servidor SMTP de origem estar inscrito em uma lista negra de spammers.

067 - Conexão SMTP recusada pelo servidor ou servidor fora do ar

Esta mensagem indica que o proxy SMTP tentou uma conexão com o servidor SMTP de destino, porem o mesmo pode ter recusado ou esta fora do ar. Verifique se o servidor destino esta no ar realizando um telnet na porta 25 do mesmo.

068 - Cliente SMTP enviou linha de tamanho excessivo

O cliente SMTP enviou uma linha de tamanho muito grande que nao pode ser tratada pelo proxy SMTP. Verifique se o cliente segue a padronização da RFC ou ajuste o mesmo para tal.

069 - Cliente SMTP fechou conexão

O cliente SMTP fechou inesperadamente a conexão. Isto pode ter acontecido por intervenção do próprio usuário ou por problemas do cliente. Normalmente as conexões são restabelecidas automaticamente.

070 - Servidor SMTP enviou linha de tamanho excessivo

O servidor SMTP enviou uma linha de tamanho muito grande que não pode ser tratada pelo proxy SMTP. Verifique se o servidor segue a padronização da RFC ou ajuste o mesmo para tal.

071 - Servidor SMTP fechou conexão

O servidor SMTP fechou inesperadamente a conexão. Isto pode ter acontecido por problemas de trafego excessivo ou erro no proprio servidor. Normalmente as conexões são restabelecidas automaticamente. Se o problema esta ocorrendo com freqüência tente aumentar os tempos de negociação do protocolo SMTP no proxy.

072 - Servidor SMTP acusou erro

Esta mensagem indica que o servidor SMTP considerou uma das transações SMTP errada.

073 - Endereço de e-mail inválido enviado pelo cliente SMTP

Esta mensagem indica que o cliente SMTP não forneceu um endereço de e-mail em formato válido.

074 - Tentativa de relay não permitido bloqueada

Esta mensagem indica que uma tentativa de relay foi bloqueada pelo firewall. Verifique o capítulo Editando os parâmetros de um contexto SMTP para liberar domínios permitidos para relay.

075 - Falta de espaço (disco cheio) para analisar mensagem

Esta mensagem indica que o disco rígido do firewall está cheio. Tente esvaziar os arquivos de logs ou aumentar a capacidade do disco para o firewall poder analisar a mensagem.

076 - Mensagem estourou tamanho máximo permitido

Esta mensagem indica que a mensagem SMTP ultrapassou o tamanho máximo permitido. Verifique o capítulo Editando os parâmetros de um contexto SMTP para aumentar o tamanho de recebimento da mensagem.

077 - Mensagem com erro de sintaxe

Esta mensagem indica que a mensagem SMTP estava com erro de sintaxe dos comandos SMTP. Geralmente programas de spammers fazem com que este erro aconteça.

078 - Anexo com vírus removido

Esta mensagem indica que um anexo da mensagem continha vírus e foi removido. O complemento da mensagem indica quem são o remetente e o destinatário da mensagem, assim como o nome do vírus encontrado.

079 - Anexo removido

Esta mensagem indica que um anexo da mensagem foi removido. O complemento da mensagem indica quem são o remetente e o destinatário da mensagem.

080 - Mensagem descartada por causa de seu anexo

Esta mensagem indica que uma mensagem tinha um anexo inaceitável (veja suas regras) e foi bloqueada pelo proxy SMTP do Firewall. O complemento da mensagem indica quem são o remetente e o destinatário da mensagem.

081 - Anexo continha vírus e foi desinfectado

Esta mensagem indica que um anexo da mensagem continha vírus e foi desinfectado. O complemento da mensagem indica quem são o remetente e o destinatário da mensagem, assim como o nome do vírus encontrado.

082 - Anexo incorretamente codificado (mensagem defeituosa)

Esta mensagem indica que um anexo de mensagem esta incorretamente codificado, ou seja apresenta erro na codificação do tipo MIME. Normalmente este arquivo pode ser descartado pelo firewall caso o administrador configure a opção desejada. Para mais informações leia o capitulo intitulado Configurando o proxy SMTP .

083 - URL aceita

Esta mensagem indica que o proxy WWW aceitou um pedido de uma URL feito por um usuário. A mensagem complementar entre parênteses indica o nome do usuário que fez a requisição. A linha de mensagem seguinte indica o endereço IP da máquina da qual a requisição se originou e a terceira linha indica qual URL foi acessada.

Esta mensagem somente será produzida para URLs do protocolo HTTP quando elas resultarem em código HTML. Para os protocolos FTP e Gopher, ela será gerada para cada requisição aceita, independente do seu tipo.

084 - Download de arquivo local aceito

Esta mensagem indica que o proxy WWW aceitou um pedido de uma URL feito por um usuário. A mensagem complementar entre parênteses indica o nome do usuário que fez a requisição. A linha de mensagem seguinte indica o endereço IP da máquina da qual a requisição se originou e a terceira linha indica qual URL foi acessada.

Esta mensagem se refere a um arquivo armazenado localmente no firewall, que foi requisitado utilizando-se o proxy WWW como um servidor WEB.

085 - URL rejeitada

Esta mensagem indica que o proxy WWW rejeitou um pedido de uma URL feito por um usuário. A mensagem complementar entre parênteses indica o nome do usuário que fez a requisição. A linha de mensagem seguinte indica o endereço IP da máquina da

qual a requisição se originou e a terceira linha indica qual URL que o usuário tentou acessar.

086 - Banner removido

Esta mensagem indica que o proxy WWW substitui uma requisição por uma imagem em branco, visto que a URL se encaixou nas regras de filtragem de banners. A mensagem complementar entre parênteses indica o nome do usuário que fez a requisição. A linha de mensagem seguinte indica o endereço IP da máquina da qual a requisição se originou e a terceira linha indica qual URL que o usuário tentou acessar.

087 - Pacote fora das regras do proxy SOCKS

Essa mensagem indica que o proxy SOCKS recebeu uma solicitação de abertura de conexão TCP ou de envio de pacote UDP e a mesma não se encaixou em nenhuma regra de filtragem do perfil de acesso correspondente. Devido a isso a solicitação foi recusada.

As mensagens complementares indicam o nome do usuário que enviou a requisição (se a autenticação de usuários estiver habilitada), o endereço do cliente, o endereço destino da requisição e seu protocolo.

088 - Pacote UDP aceito pelo proxy SOCKS

Essa mensagem indica que o proxy SOCKS recebeu uma solicitação de envio de um pacote UDP e o mesmo foi enviado, devido a existência de uma regra no perfil de acesso correspondente indicando que o proxy poderia fazê-lo.

As mensagens complementares indicam o nome do usuário que enviou o pacote (se a autenticação de usuários estiver habilitada), o endereço do cliente e o endereço destino.

089 - Pacote UDP recusado pelo proxy SOCKS

Essa mensagem indica que o proxy SOCKS recebeu uma solicitação de envio de um pacote UDP e o mesmo foi recusado, devido a existência de uma regra no perfil de acesso correspondente indicando que o proxy não deveria aceitar tal requisição.

As mensagens complementares indicam o nome do usuário que tentou enviar o pacote (se a autenticação de usuários estiver habilitada), o endereço do cliente e o endereço destino.

090 - Conexão TCP estabelecida através do proxy SOCKS

Essa mensagem indica que o proxy SOCKS recebeu uma solicitação de estabelecimento de uma conexão TCP e a mesmo foi estabelecida, devido a existência de uma regra no perfil de acesso correspondente indicando que o proxy poderia fazê-lo.

As mensagens complementares indicam o nome do usuário que estabeleceu a conexão (se a autenticação de usuários estiver habilitada), o endereço do cliente e o endereço para o qual a conexão foi estabelecida.

091 - Conexão TCP finalizada através do proxy SOCKS

Essa mensagem é gerada todas as vezes que uma conexão TCP é finalizada através do proxy SOCKS.

As mensagens complementares indicam o nome do usuário que havia estabelecido a conexão (se a autenticação de usuários estiver habilitada), o endereço do cliente e o endereço para o qual a conexão foi estabelecida.

092- Conexão TCP recusada pelo proxy SOCKS

Essa mensagem indica que o proxy SOCKS recebeu uma solicitação de estabelecimento de uma conexão TCP e a mesmo foi recusada, devido a existência de uma regra no perfil de acesso correspondente indicando que o proxy não deveria aceitar tal conexão.

As mensagens complementares indicam o nome do usuário que solicitou a conexão (se a autenticação de usuários estiver habilitada), o endereço do cliente e o endereço de destino.

093 - Dados incorretos recebidos pelo proxy SOCKS

Essa mensagem é gerada quando o proxy SOCKS recebe dados do cliente em desacordo com a especificação do protocolo SOCKS. Exemplos de dados inválidos podem ser uma versão do protocolo diferente de 4 ou 5, um endereço destino em branco, entre outros.

094 - Erro ao comunicar com servidor de autenticação

Esta mensagem indica que um dos proxies não conseguiu se comunicar com o servidor de autenticação quando tentou realizar a autenticação de um usuário. Devido a isso, o usuário não foi autorizado a continuar e a sua conexão foi recusada.

Solução: Verifique se o processo do servidor de autenticação está ativo no firewall. Para fazer isso, execute o comando

#**`ps -ax | grep fwauthd | grep -v grep`**. Caso o processo não apareça, execute-o com o comando **`/etc/firewall/fwauthd`**. Se o processo estiver ativo ou se este problema voltar a ocorrer, contate o suporte técnico.

095 - Erro ao conectar com agente de autenticação

Esta mensagem indica que o servidor de autenticação não conseguiu se conectar o agente de autenticação que estaria rodando em uma determinada máquina. A mensagem complementar indica o nome do agente de autenticação que não pode ser conectado e o endereço IP que ele supostamente estaria rodando.

Solução: Verifique se o endereço IP da máquina onde o agente estaria rodando está correto na definição do autenticador (para maiores informações, veja o capítulo intitulado Cadastrando Entidades) e que o agente está realmente sendo executado na máquina em questão.

096 - Erro de comunicação com agente de autenticação

Esta mensagem indica que o servidor de autenticação conseguiu se conectar ao agente de autenticação porém não conseguiu estabelecer uma comunicação. A mensagem complementar indica o nome do agente de autenticação que provocou o problema.

Solução: Verifique se a senha de acesso na definição do autenticador está igual a senha colocada na configuração do agente de autenticação. Para maiores informações, veja o capítulo intitulado Cadastrando Entidades.

097 - Erro ao conectar com agente IDS

Esta mensagem indica que o firewall não conseguiu se conectar ao agente IDS que estaria rodando em uma determinada máquina. A mensagem complementar indica o nome do agente IDS que não pode ser conectado e o endereço IP que ele supostamente estaria rodando.

Solução: Verifique se o endereço IP da máquina onde o agente estaria rodando está correto na definição da entidade (para maiores informações, veja o capítulo intitulado Cadastrando Entidades) e que o agente está realmente sendo executado na máquina em questão.

098 - Erro de comunicação com agente IDS

Esta mensagem indica que o firewall conseguiu se conectar ao agente IDS porém não conseguiu estabelecer uma comunicação. A mensagem complementar indica o nome do agente IDS que provocou o problema e o endereço IP da máquina onde ele está rodando.

Solução: Verifique se a senha de acesso na definição da entidade está igual a senha colocada na configuração do agente IDS. Para maiores informações, veja o capítulo intitulado Cadastrando Entidades.

099 - Regra de bloqueio IDS acrescentada

Esta mensagem indica que o agente de detecção de intrusão acrescentou uma regra de bloqueio temporária no firewall em decorrência de algum evento.

As mensagens complementares indicam que tipo de bloqueio foi acrescentado (origem, destino e/ou serviço) e os endereços e/ou serviço bloqueados.

100 - Erro ao conectar com servidor de anti-vírus

Esta mensagem indica que o firewall não conseguiu se conectar ao servidor de anti-vírus que estaria rodando em uma determinada máquina. A mensagem complementar indica o nome do servidor que não pode ser conectado e o endereço IP que ele supostamente estaria rodando.

Solução: Verifique se o endereço IP da máquina onde o agente estaria rodando está correto na definição da entidade (para maiores informações, veja o capítulo intitulado

Cadastrando Entidades) e que o agente está realmente sendo executado na máquina em questão.

101 - Erro de comunicação com servidor de anti-vírus

Esta mensagem indica que o firewall conseguiu se conectar ao servidor de anti-vírus porém não conseguiu estabelecer uma comunicação. A mensagem complementar indica o nome do agente anti-vírus que provocou o problema e o endereço IP da máquina onde ele está rodando.

Solução: Verifique se a senha de acesso na definição da entidade está igual a senha colocada na configuração do agente anti-vírus. Para maiores informações, veja o capítulo intitulado Cadastrando Entidades.

102 - Erro ao conectar com analisador de URLs

Esta mensagem indica que o firewall não conseguiu se conectar ao analisador de URLs que estaria rodando em uma determinada máquina. A mensagem complementar indica o nome do analisador que não pode ser conectado e o endereço IP que ele supostamente estaria rodando.

Solução: Verifique se o endereço IP da máquina onde o analisador estaria rodando está correto na definição da entidade (para maiores informações, veja o capítulo intitulado Cadastrando Entidades) e que ele está realmente sendo executado na máquina em questão.

103 - Erro de comunicação com analisador de URLs

Esta mensagem indica que o firewall conseguiu se conectar ao analisador de URLs porém não conseguiu estabelecer uma comunicação. A mensagem complementar indica o nome do analisador que provocou o problema e o endereço IP da máquina onde ele está rodando.

Solução: Verifique se a senha de acesso na definição da entidade está igual a senha colocada na configuração do analisador de URLs. Para maiores informações, veja o capítulo intitulado Cadastrando Entidades.

104 - Nova maquina detectada no cluster

Esta mensagem indica que uma nova maquina foi anexada ao sistema de cluster do firewall

105 - Maquina participante do cluster fora do ar

Esta mensagem indica que uma das maquinas participantes do cluster esta fora do ar. Verifique a situação da maquina de modo a solucionar o problema da mesma.

106 - Pacote de heartbeat invalido

Esta mensagem indica que um pacote de verificação do cluster foi recebido incorretamente. Verifique se o segmento de comunicação dos firewall esta funcionando corretamente.

107 - Convergência do cluster completada com sucesso

Esta mensagem indica que todos os firewalls do cluster estão funcionando corretamente.

108 - Chave de ativação do firewall repetida

Esta mensagem indica que dois firewalls possuem a mesma licença instalada. Para o trabalho dos firewalls cooperativos e necessário que cada um dos firewalls possua a sua própria licença

109 - Falha de autenticação para proxy

Esta mensagem indica que um usuário informou uma senha inválida ao tentar se autenticar em um determinado proxy. As mensagens complementares indicam o nome do usuário e as máquinas de origem e destino (no caso de proxy transparente) da conexão.

110 - Usuário não cadastrado para proxy

Esta mensagem indica que um usuário não cadastrado tentou se autenticar em um determinado proxy. A mensagem complementar indica as máquinas de origem e destino (no caso de proxy transparente) da conexão.

111 - Usuário sem permissão para telnet

Esta mensagem indica que um usuário se autenticou corretamente no proxy telnet porém não tinha permissão de efetuar a conexão desejada. As mensagens complementares indicam o nome do usuário e as máquinas de origem e destino da conexão.

112 - Sessão telnet estabelecida

Esta mensagem indica que um usuário se autenticou corretamente no proxy telnet e tinha permissão para efetuar a conexão desejada. Devido a isso, a conexão foi estabelecida. As mensagens complementares indicam o nome do usuário e as máquinas de origem e destino da conexão.

113 - Sessão telnet finalizada

Esta mensagem indica que um usuário se desconectou de uma sessão telnet. As mensagens complementares indicam o nome do usuário e as máquinas de origem e destino da conexão.

114 - Erro ao enviar dados para o kernel do Firewall

Esta mensagem indica que algum dos módulos externos tentou enviar informações para os módulos do firewall que rodam dentro do kernel e não conseguiu. Se existir uma

mensagem complementar entre parênteses, esta indicará quais informações estavam sendo enviadas.

Solução: Verifique se o módulo do Firewall Aker está carregado no kernel. No FreeBSD utilize o comando **kldstat** e no Linux o comando **lsmod**. Em ambos os casos deverá aparecer um módulo com o nome **aker_firewall_mod**.

115 - Erro ao salvar certificados

Esta mensagem indica que o firewall não conseguiu salvar alguma lista de certificados de criptografia no disco.

Solução: Verifique se o existe espaço disponível no diretório '/' do firewall. Isto pode ser feito através do comando **"$df -k"**. Se este comando mostrar o diretório '/' com 100% de espaço utilizado, então é isto a causa do problema. Caso exista espaço disponível e ainda assim este erro apareça, consulte o suporte técnico.

116 - Erro ao carregar certificados

Esta mensagem indica que o firewall não conseguiu carregar alguma lista de certificados de criptografia.

Solução: Contate o suporte técnico

117 - Certificado inválido recebido

Esta mensagem indica que o servidor de certificados do firewall recebeu um certificado inválido. Isso pode ter uma das seguintes causas:

- Assinatura do certificado inválida
- Entidade certificadora desconhecida
- Certificado expirado

As mensagens complementares indicam qual destes possíveis erros ocorreu e qual firewall emitiu o certificado inválido.

118 - Certificado recebido e validado corretamente

Esta mensagem indica que o servidor de certificados do firewall recebeu um certificado de negociação ou revogação válido. As mensagens complementares indicam que tipo de certificado foi recebido e qual firewall o emitiu.

119 - Requisição de cliente de criptografia inválida

Esta mensagem indica que o servidor de certificados recebeu uma requisição de um cliente de criptografia e esta requisição foi considerada inválida. Isso pode ter uma das seguintes causas:

- O certificado do firewall foi atualizado e o cliente continua utilizando o certificado antigo

- A requisição partiu de uma máquina não autorizada a estabelecer sessão de criptografia com o firewall

As mensagens complementares indicam qual a causa do problema e os endereços da máquina de origem e destino (o destino é o endereço da máquina atrás do firewall com a qual o cliente tentou se comunicar).

120 - Falha de autenticação para criptografia

Esta mensagem só é mostrada quando a autenticação de usuários para clientes de criptografia está ativa e indica que um usuário cadastrado em algum autenticador tentou estabelecer uma sessão de criptografia com o firewall porém sua senha estava incorreta. As mensagens complementares mostram o nome do usuário em questão e os endereços da máquina de origem e destino (o destino é o endereço da máquina atrás do firewall com a qual o cliente tentou se comunicar).

121 - Usuário não cadastrado para criptografia

Esta mensagem só é mostrada quando a autenticação de usuários para clientes de criptografia está ativa e indica que um usuário não cadastrado em nenhum autenticador tentou estabelecer uma sessão de criptografia com o firewall. A mensagem complementar mostra os endereços da máquina de origem e destino (o destino é o endereço da máquina atrás do firewall com a qual o cliente tentou se comunicar).

122 - Sessão de criptografia com cliente estabelecida

Esta mensagem é gerada pelo servidor de certificados quando um usuário consegue se autenticar corretamente em um cliente de criptografia e iniciar uma sessão. Nas mensagens complementares é mostrado o login do usuário que estabeleceu a sessão e os endereços da máquina de origem e destino (o destino é o endereço da máquina atrás do firewall com a qual o cliente se comunicou inicialmente).

123 - Sessão de criptografia com cliente finalizada

Esta mensagem indica que um cliente finalizou uma sessão criptografada. A mensagem complementar indica a máquinas de origem da conexão.

124 - Erro de comunicação com cliente de criptografia

Esta mensagem, que pode ter várias causas, indica que o servidor de criptografia para clientes recebeu um pacote criptografado inválido de um Cliente de Criptografia Aker.

As mensagens complementares indicam qual a causa do problema e os endereços da máquina de origem e destino (o destino é o endereço da máquina atrás do firewall com a qual o cliente tentou se comunicar).

125 - Erro ao carregar algoritmo de criptografia

O Firewall Aker pode trabalhar com algoritmos de criptografia desenvolvidos por terceiros, chamados de algoritmos externos. Esta mensagem indica que o servidor de

criptografia para clientes não conseguiu carregar um destes algoritmos de criptografia externos. Isto é causado por uma falha de implementação do algoritmo.

As mensagens complementares mostram o nome da biblioteca a partir da qual o firewall tentou carregar o algoritmo e o erro que causou o problema.

Solução: Contate o desenvolvedor do algoritmo e repasse a mensagem completa para ele.

126 - Falha de autenticação para perfil de acesso

Esta mensagem indica que um usuário informou uma senha inválida ao tentar se logar no firewall utilizando o Cliente de Autenticação Aker. As mensagens complementares indicam o nome do usuário e a máquina de origem da requisição.

127 - Usuário não cadastrado para perfil de acesso

Esta mensagem indica que um usuário não cadastrado tentou se logar no firewall utilizando o Cliente de Autenticação Aker. A mensagem complementar indica a máquina de origem da requisição.

128 - Sessão de perfil de acesso estabelecida

Esta mensagem indica que um usuário se logou corretamente no firewall utilizando o Cliente de Autenticação Aker. As mensagens complementares indicam o nome do usuário que estabeleceu a sessão e a máquina a partir da qual a sessão foi estabelecida.

129 - Sessão de perfil de acesso finalizada

Esta mensagem indica que um usuário finalizou um sessão no firewall estabelecida através do Cliente de Autenticação Aker. As mensagens complementares indicam o nome do usuário que finalizou a sessão e a máquina a partir da qual a sessão foi finalizada.

130 - Requisição de perfil de acesso inválida

Esta mensagem, que pode ter várias causas, indica que o servidor de login de usuários recebeu uma requisição inválida de um Cliente de Autenticação Aker.

As mensagens complementares indicam qual a causa do problema e o endereço da máquina de origem da requisição.

131 - Erro ao carregar pseudo-grupos

Esta mensagem indica que o firewall não conseguiu carregar a lista de pseudo-grupos das autoridades certificadoras.

Solução: Contate o suporte técnico

132 - Erro ao baixar CRL

Essa mensagem indica que o firewall não conseguiu baixar a lista de certificados revogados (CRL) de uma autoridade certificadora. As mensagens complementares mostram a razão pela qual não foi possível baixar a lista e a URL da qual se tentou baixá-la.

Solução: Verifique que a URL informada na definição da entidade do tipo autoridade certificadora está correta e que o serviço está no ar. É possível fazer isso digitando-se a URL em um browser e verificando se é possível se receber o arquivo.

133 - Número de processos excessivo no sistema

Esta mensagem indica que algum dos módulos externos do firewall, ao tentar criar uma nova instância de si próprio para tratar uma conexão, detectou que o número de processos executando no sistema está próximo do limite máximo permitido. Diante disso, a criação do novo processo foi cancelada e a conexão que deveria ser tratada pelo novo processo foi abortada.

Solução: Aumente o número máximo de processos no sistema. Para maiores informações, consulte o Apêndice B - Perguntas e respostas.

134 - Máquina de conversão 1-N fora do ar

Essa mensagem indica que uma das máquinas participantes de uma conversão 1-N (balanceamento de canal) se encontra fora do ar. A mensagem complementar mostra o endereço IP da máquina em questão.

135 - Máquina de conversão 1-N operacional

Essa mensagem indica que uma das máquinas participantes de uma conversão 1-N (balanceamento de canal) que se encontrava fora do ar voltou a funcionar normalmente. A mensagem complementar mostra o endereço IP da máquina em questão.

136 - Pedido de conexão de administração

Esta mensagem é gerada pelo módulo de administração remota do Firewall Aker todas as vezes que este recebe um pedido de abertura de conexão. Na mensagem complementar é mostrado o endereço IP da máquina que solicitou a abertura de conexão.

137 - Sessão de administração estabelecida

Esta mensagem é gerada pelo módulo de administração remota do Firewall Aker quando um usuário consegue se autenticar corretamente e iniciar uma sessão de administração. Na mensagem complementar é mostrado o login do usuário que estabeleceu a sessão e os seus direitos.

Os direitos do usuário são representados através de três siglas independentes. Caso o usuário possua um determinado direito será mostrada a sigla correspondente a ele, caso contrário será mostrado o valor "--". As siglas e seus significados são os seguintes:

- **CF** - Configura Firewall
- **CL** - Configura Log
- **GU** - Gerencia usuários

138 - Sessão de administração finalizada

Esta mensagem indica que a sessão de administração estabelecida anteriormente foi terminada a pedido do cliente.

139 - Usuário não cadastrado para administração

Esta mensagem indica que um usuário não cadastrado no sistema tentou estabelecer uma sessão de administração.

140 - Erro de confirmação de sessão de administração

Esta mensagem indica que um usuário cadastrado no sistema tentou estabelecer uma sessão de administração remota porém sua senha estava incorreta. A mensagem complementar mostra o nome do usuário em questão.

141 - Firewall sendo administrado por outro usuário

Esta mensagem indica que um usuário conseguiu se autenticar corretamente para estabelecer uma sessão de administração remota, porém já existia um outro usuário com uma sessão aberta para a mesma máquina e por isso a conexão foi recusada. A mensagem complementar indica qual o usuário que teve sua sessão recusada.

142 - Alteração de parâmetro

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou algum parâmetro de configuração do sistema. A mensagem complementar indica o nome do parâmetro que foi alterado.

143 - Alteração das regras de filtragem

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou a tabela de regras de filtragem do firewall.

144 - Alteração da conversão

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou algum parâmetro da conversão de endereços ou a tabela de conversão de servidores. A mensagem complementar indica exatamente o que foi alterado.

145 - Alteração da tabela de criptografia

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou a tabela de criptografia do firewall.

146 - Alteração na configuração de SYN Flood

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou algum parâmetro da proteção contra SYN Flood. A mensagem complementar indica exatamente o que foi alterado.

147 - Alteração de contextos

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou contextos de um dos proxies transparentes do Firewall. A mensagem complementar indica qual o proxy que teve seus contextos modificados.

148 - Alteração da configuração de SNMP

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou os parâmetros de configuração do agente SNMP.

149 - Alteração dos perfis de acesso

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou a lista de perfis de acesso.

150 - Alteração da lista de controle de acesso

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou a lista de controles de acesso.

151 - Alteração de parâmetros de autenticação

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou os parâmetros globais de autenticação.

152 - Alteração de entidades

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou a lista de entidades do sistema.

153 - Alteração de parâmetros WWW

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou os parâmetros WWW.

154 - Alteração da configuração do proxy SOCKS

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou algum dos parâmetros de configuração do proxy SOCKS.

155 - Remoção de conexão ativa

Esta mensagem indica que o administrador que estava com a sessão de administração aberta removeu uma das conexão ativas. A mensagem complementar indica se a conexão removida era TCP ou UDP.

156 - Remoção de sessão de usuário ativa

Esta mensagem indica que o administrador que estava com a sessão de administração aberta removeu uma das sessões de usuários que estavam logados no firewall através do Cliente de Autenticação Aker.

157 - Operação sobre o arquivo de log

Esta mensagem indica que o administrador que estava com a sessão de administração aberta realizou uma operação sobre o arquivo de log. As operações possíveis são *Compactar* e *Apagar*. A mensagem complementar indica qual destas operações foi executada.

158 - Operação sobre o arquivo de eventos

Esta mensagem indica que o administrador que estava com a sessão de administração aberta realizou uma operação sobre o arquivo de eventos. As operações possíveis são *Compactar* e *Apagar*. A mensagem complementar indica qual destas operações foi executada.

159 - Operação sobre o arquivo de usuários

Esta mensagem indica que o administrador que estava com a sessão de administração aberta realizou uma operação sobre o arquivo de usuários. As operações possíveis são *Incluir*, *Excluir* e *Alterar*. A mensagem complementar indica qual destas operações foi executada e sobre qual usuário.

160 - Alteração na data/hora do firewall

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou a data e/ou a hora do firewall.

161 - Carga do certificado de negociação local

Esta mensagem indica que o administrador que estava com a sessão de administração aberta carregou ou alterou o certificado de negociação local do firewall.

162 - Alteração nos certificados

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou a lista de certificados das entidades certificadoras ou de revogação do firewall.

163 - Alteração da configuração de TCP/IP

Esta mensagem indica que o administrador que estava com a sessão de administração aberta alterou a configuração de TCP/IP do firewall (hostname, configuração de DNS, configuração de interfaces ou rotas).

164 - Queda de sessão de administração por erro

Esta mensagem indica que a sessão de administração que estava ativa foi interrompida devido a um erro de protocolo de comunicação.

Solução: Experimente estabelecer a conexão novamente. Se o problema voltar a ocorrer, consulte o suporte técnico.

165 - Queda de sessão de administração por inatividade

Quando uma interface remota estabelece uma conexão de administração, ela passa a enviar periodicamente pacotes para o firewall indicando que ela continua ativa. Estes pacotes são enviados mesmo que usuário não execute nenhuma operação.

Esta mensagem indica que a sessão de administração que estava ativa foi interrompida devido a um tempo limite ter sido atingido, sem o servidor ter recebido nenhum pacote da interface remota. A sua causa mais provável é uma queda na máquina que rodava a interface gráfica ou uma queda na rede.

166 - Erro na operação anterior

Esta mensagem indica que a última operação executada pelo servidor de comunicação remota não foi executada com sucesso.

Solução: Verifique se o existe espaço disponível no diretório '/' do firewall. Isto pode ser feito através do comando **"$df -k"**. Se este comando mostrar o diretório '/' com 100% de espaço utilizado, então é isto a causa do problema. Caso exista espaço disponível e ainda assim este erro apareça, consulte o suporte técnico.

167 - Usuário sem direito de acesso

Esta mensagem indica que o usuário tentou realizar uma operação que não lhe era permitida.

Solução: Esta mensagem não deve ser mostrada em condições normais de funcionamento do Firewall Aker. Se ela aparecer, contate o suporte técnico.

168 - Pacote não reconhecido

Esta mensagem indica que o servidor de comunicação do firewall recebeu uma requisição de serviço desconhecida.

Solução: Contate o suporte técnico.

169 - Muitas negociações pendentes

Esta mensagem indica que o kernel não está conseguindo pedir que o daemon de negociações de chave estabeleça um canal. Esta situação é anômala e não deve acontecer. Por favor contate o suporte técnico se o Firewall gerar esta mensagem.

170 - SA não tem tipo IPSEC

Esta mensagem indica que foi tentada a configuração de um canal não IPSEC pelo módulo IPSEC. Esta situação é anômala e não deve acontecer. Por favor contate o suporte técnico se o Firewall gerar esta mensagem.

171 - Algoritmo de criptografia especificado não implementado

Esta mensagem indica que foi negociado um canal de criptografia com um algoritmo não implementado. Escolha outros algoritmos (veja seção Configurando canais Firewall-Firewall).

172 - Falhou a expansão da chave criptográfica

Esta mensagem indica que o módulo IPSEC teve dificuldades em tratar a chave negociada para um canal criptográfico. Esta situação é anômala e não deve acontecer. Por favor contate o suporte técnico se o Firewall gerar esta mensagem.

173 - Kernel repassou pacote inválido

Esta mensagem indica que o sistema operacional passou um pacote incorreto para o Firewall. Ela ocorre apenas no sistema operacional Linux.

174 - Falhou ao inserir SA no kernel

Esta mensagem indica que foi negociado um canal que já não existe mais. Para solucionar o problema, recrie o canal, ou aguarde até que todos os módulos do Firewall saibam da não existência deste canal.

175 - Estabelecendo VPN IPSEC para o tráfego

Esta mensagem indica que o daemon de negociação de chaves IPSEC (fwiked) iniciou o estabelecimento de um canal, por necessidade imediata de seu uso.

176 - fwiked falhou ao iniciar

Esta mensagem indica que o daemon de negociação de chaves IPSEC (fwiked) não conseguiu ler suas configurações. Recrie as configurações de criptografia para solucionar o problema (veja seção Configurando canais Firewall-Firewall).

177 - Erro processando configuração

Esta mensagem indica que ocorreu um erro interno grave no daemon de negociação de chaves IPSEC (fwiked). Esta situação é anômala e não deve acontecer. Por favor contate o suporte técnico se o Firewall gerar esta mensagem.

178 - Erro comunicando com o kernel

Esta mensagem indica que o daemon de negociação de chaves IPSEC (fwiked) não está conseguindo se comunicar com os módulos do Firewall que executam dentro do kernel do sistema operacional.

179 - Kernel enviou requisição incorreta

Esta mensagem indica que o daemon de negociação de chaves IPSEC (fwiked) recebeu uma solicitação para negociar um canal de criptografia que não mais existe na configuração do Firewall. Espere alguns instantes até que todos os módulos do Firewall se sincronizem.

180 - Tentou instalar uma SA não negociada

Esta mensagem indica que o daemon de negociação de chaves IPSEC (fwiked) encontrou um erro grave de consistência interna. Esta situação é anômala e não deve acontecer. Por favor contate o suporte técnico se o Firewall gerar esta mensagem.

181 - Algoritmo criptográfico não suportado

Esta mensagem indica que um outro Firewall (ou qualquer equipamento que suporte IPSEC) tentou estabelecer um canal criptográfico com um algoritmo de cifração não suportado pelo Firewall Aker. Escolha outros algoritmos (veja seção Configurando canais Firewall-Firewall).

182 - Erro enviando regra de ike ao filtro de pacotes

Esta mensagem indica que o daemon de negociação de chaves IPSEC (fwiked) não está conseguindo se comunicar com os módulos do Firewall que executam dentro do kernel do sistema operacional para inserir uma regra de liberação da comunicação com seus pares.

183 - Sucesso ativando a SA negociada

Esta mensagem indica que o daemon de negociação de chaves IPSEC (fwiked) estabeleceu e instalou nos demais módulos do Firewall um canal de criptografia IPSEC corretamente.

184 - Negociação de IKE falhou (olhar mensagens complementares)

Esta mensagem indica que houve um problema durante a negociação de chaves IPSEC. Verifique as mensagens complementares para obter mais detalhes.

Geralmente uma pequena mudança de configuração resolve rapidamente o problema.

185 - Erro lendo mudanca de estado do cluster

Esta mensagem indica que houve um erro quando da leitura do estado do cluster dentro do trabalho cooperativo. Verifique o segemento de rede onde estao instalados os firewalls.

186 - Erro enviando mudanca de estado ao cluster

Esta mensagem indica que houve um erro quando enviando mudanca do estado do cluster dentro do trabalho cooperativo. Verifique o segemento de rede onde estao instalados os firewalls.

187 - Notificação do fwiked (olhar mensagens complementares)

Estam mensagem é uma mensagem genérica de **notificação** do daemon de negociação de chaves IPSEC. Verifique as mensagens complementares para obter mais detalhes.

188 - Aviso do fwiked (olhar mensagens complementares)

Estam mensagem é uma mensagem genérica de **aviso** do daemon de negociação de chaves IPSEC. Verifique as mensagens complementares para obter mais detalhes.

189 - Recebendo número do pipe do kernel

Esta mensagem indica que um proxy não conseguiu descobrir quais eram o pipe e o acumulador para uma conexão, visto que tiveram problemas de comunicação com o Kernel.

190 - Erro lendo arquivo de configuração de estatísticas

Esta mensagem indica que houve um problema ao ler o arquivo de configuração de estatísticas. A solução é restaurá-lo ou removê-lo e criar as configurações novamente. Veja a seção Arquivos do Sistema e Backup.

191 - Erro lendo tabela de entidades

Esta mensagem indica que o módulo gerador de estatísticas do Firewall não conseguiu não conseguiu ler a tabela de entidades do sistema.

192 - Não encontrou entidade acumulador

Esta mensagem indica que o módulo gerador de estatísticas do Firewall encontrou uma inconsistência em sua configuração, isto é, uma estatística que referencia um acumulador inexistente. A mensagem complementar entre parênteses indica qual a entidade em questão

193 - Daemon suspenso por configuração incorreta

Esta mensagem indica que o módulo gerador de estatísticas do Firewall encontrou uma inconsistência em sua configuração e ficará com suas atividades suspensas até que ela esteja correta.

194 - Erro recebendo estatísticas do kernel

Esta mensagem indica que o módulo gerador de estatísticas do Firewall teve problemas ao ler os dados necessários ao seu cálculo dos módulo que executam dentro do kernel do sistema operacional.

195 - Erro salvando estatísticas

Esta mensagem indica que o módulo gerador de estatísticas do Firewall teve problemas ao armazenar os dados coletados (ou enviá-los ao servidor de log remoto). Se o log for local, verifique a possibilidade de o disco estar cheio. Se for remoto, verifique a correta conexão com o servidor de log remoto.

196 - Erro recebendo período máximo de permanência das estatísticas

Esta mensagem indica que o módulo gerador de estatísticas do Firewall não conseguiu ler o período máximo pelo qual deve manter as estatísticas no Firewall (apenas para log local).

197 - Pedido de fluxo inexistente

Esta mensagem indica que uma incosistência interna ocorreu, de forma que um fluxo de dados para controle de banda (QoS), não foi encontrado.

198 - Pedido de pipe inexistente

Esta mensagem indica que uma incosistência interna ocorreu, de forma que um pipe para controle de banda (QoS), não foi encontrado.

199 - Apagando registros do sistema de log

Esta mensagem indica que os registros do sistema de log foram apagados. A mensagem complementar entre parênteses informa se foram apagados logs, estatísticas ou eventos.

200 - Erro executando shell

Esta mensagem informa que um erro grave de configuração foi encontrado que impede o login no console do Firewall Box. Contate o suporte técnico de seu revendedor.

201 - Erro lendo licença

Esta mensagem indica que as informações de licença do Firewall estão com algum problema sério que impedem sua leitura. Reinsira a chave de ativação no Firewall.

202 - Tentativa de login (console) frustada por senha incorreta

Esta mensagem indica que alguém tentou efetuar login no console do Firewall Box, mas não tinha a senha correta.

203 - Sistema com defeito irremediável. Contate o revendedor

Esta mensagem informa que um erro grave de configuração foi encontrado que impede o login no console do Firewall Box. Contate o suporte técnico de seu revendedor.

204 - Login no console efetuado

Esta mensagem registra o fato de algum operador ter efetuado login no console do Firewall Box.

205 - Linha de resposta muito grande

Esta mensagem indica que o proxy POP3 transparente recebeu uma linha de resposta demasiado grande. Veja a RFC 1939 para maiores informações.

206 - Erro recebendo dados do servidor POP3

Esta mensagem indica que o proxy POP3 transparente encontrou um erro de conexão ao receber dados do servidor. As mensagens complementares informam qual a conexão em questão.

207 - Erro recebendo dados do cliente POP3

Esta mensagem indica que o proxy POP3 transparente encontrou um erro de conexão ao receber dados do cliente. As mensagens complementares informam qual a conexão em questão.

208 - Erro enviando dados ao cliente POP3

Esta mensagem indica que o proxy POP3 transparente encontrou um erro de conexão ao enviar dados para o cliente. As mensagens complementares informam qual a conexão em questão.

209 - Erro enviando dados ao servidor POP3

Esta mensagem indica que o proxy POP3 transparente encontrou um erro de conexão ao enviar dados ao servidor. As mensagens complementares informam qual a conexão em questão.

210 - Resposta inválida do servidor POP3

Esta mensagem indica que o proxy POP3 transparente recebeu uma resposta incorreta do servidor. As mensagens complementares informam que resposta foi esta

211 - Erro conectando-se ao servidor POP3

Esta mensagem indica que o proxy POP3 transparente não consegui estabelecer a conexão com o servidor. Provavelmente o endereço está errado ou o servidor está fora do ar.

212 - Servidor POP3 recusou a conexão

Esta mensagem indica que o proxy POP3 transparente conectou-se ao servidor e este informou estar fora do ar.

213 - Comando POP3 inválido ou erro de sintaxe

Esta mensagem indica que o proxy POP3 transparente leu um comando incorreto do cliente e fechou a conexão sem repassá-lo ao servidor. O comando em questão encontra-se nas mensagens complementares.

214 - Erro abrindo arquivo para spool

Esta mensagem indica que o proxy POP3 transparente não conseguiu abrir o arquivo temporário para salvar a mensagem

215 - Erro gravando dados no arquivo

Esta mensagem indica que o proxy POP3 transparente encontrou um erro ao gravar a mensagem em espaço de armazenamento temporário.

216 - Falta de espaço gravando arquivo

Esta mensagem indica que faltou espaço em disco para o proxy POP3 transparente gravar as mensagens recebidas.

217 - Erro de sintaxe no email POP3 (erro de parser)

Esta mensagem indica que o proxy POP3 transparente recebeu uma mensagem incorretamente formatada e a descartou por não poder analisá-la.

218 - Entrando em modo STLS - nenhuma analise possível

Esta mensagem indica que o firewall entrou em modo STLS. Entre em contato com o suporte técnico para a solução.

219 - Erro recebendo dados do firewall servidor

Esta mensagem indica que o firewall servidor do cluster não esta recebendo os dados corretamente. Verifique o segmento de rede de troca informação dos firewalls cooperativos.

220 - Erro enviando dados do firewall servidor

Esta mensagem indica que o firewall servidor do cluster não esta enviando os dados corretamente. Verifique o segmento de rede de troca informação dos firewalls cooperativos.

221 - Erro de processamento no firewall servidor

Esta mensagem indica que o firewall servidor do cluster não esta processando os dados corretamente. Verifique o firewall servidor quanto a espaço em disco e processador.

222 - Erro alterando a configuração do firewall

Esta mensagem indica que o firewall servidor do cluster não esta conseguindo alterar as configurações dos outros firewalls. Verifique o segmento de rede de troca informação dos firewalls cooperativos.

223 - Erro ao replicar estado do cluster

Esta mensagem indica que o firewall servidor do cluster não esta conseguindo replicar o estado do cluster para os outros firewalls. Verifique o segmento de rede de troca informação dos firewalls cooperativos.

224 - Erro ao enviar arquivo ao cluster

Esta mensagem indica que o firewall servidor do cluster nao esta conseguindo enviar arquivo ao cluster. Verifique o segmento de rede de troca informação dos firewalls cooperativos.

225 - Erro ao agrupar dados do cluster

Esta mensagem indica que o firewall servidor do cluster não esta conseguindo agrupar os dados do cluster. Verifique o segmento de rede de troca informação dos firewalls cooperativos.

226 - Arquivo com vírus desinfectado

Esta mensagem indica que um arquivo analisado pelo firewall estava com vírus mas foi desinfectado.

227 - Arquivo com vírus bloqueado

Esta mensagem indica que um arquivo estava com vírus e não pode ser removido, por isso o arquivo foi bloqueado.

228 - Arquivo não pode ser analisado pois estava corrompido

Esta mensagem indica que o antivírus do firewall não pode analisar o arquivo pois o mesmo estava corrompido.

229 - Arquivo não pode ser analisado pois estava cifrado

Esta mensagem indica que o antivírus do firewall não pode analisar o arquivo pois o mesmo estava cifrado.

230 - Host respondeu e foi marcado como ativo

Esta mensagem indica que a maquina de teste do balanceamento de link esta no ar. Para maiores informações consulte o capitulo intitulado Configurando a Conversão de Endereços .

231 - Host não respondeu e foi marcado como inativo

Esta mensagem indica que a maquina de teste do balanceamento de link esta fora ar ou não foi possível a sua verificação. Para maiores informações consulte o capítulo intitulado Configurando a Conversão de Endereços .

232 - Link foi marcado como ativo

Esta mensagem indica que o balanceamento de link esta no ar. Para maiores informações consulte o capitulo intitulado Configurando a Conversão de Endereços .

233 - Link foi marcado como inativo

Esta mensagem indica que o balanceamento de link esta fora do ar. Para maiores informações consulte o capitulo intitulado Configurando a Conversão de Endereços .

Apêndice B - Perguntas e respostas

Filtro com estado

Estou tentando fazer uma transferência de arquivos via FTP a partir da máquina onde o firewall está instalado. Eu consigo me conectar e ser validado pelo servidor FTP remoto, porém quando tento transferir um arquivo recebo uma mensagem de que não foi possível abrir conexão de dados. Como posso resolver este problema ?

A única maneira de se fazer uma transferência de arquivos via FTP a partir do firewall é utilizar a forma passiva. Para isso, basta digitar o comando **`passive`** na linha de comandos do FTP, logo após ser validado pelo servidor remoto. A partir deste momento, todas as transferências de arquivos serão realizadas com sucesso.

Obs: Os browsers já utilizam a forma passiva como padrão para todas as transferências de arquivos via FTP.

Administração remota

Eu estou utilizando a administração remota através da Internet. Existe algum risco da minha senha ser interceptada ?

Não. Em nenhum momento a senha de um usuário é enviada pela rede decriptada.
O método de autenticação é feito através de desafio-resposta, onde o firewall consegue autenticar o usuário sem receber a sua senha e a interface remota consegue ter certeza de que está falando com o firewall.

Eu perdi a senha do único administrador que estava cadastrado no sistema. Existe alguma maneira de recuperá-la ?

Não existe nenhuma maneira de recuperar uma senha perdida, entretanto é possível se usar um módulo local de administração de usuários e criar um outro administrador ou alterar a senha do administrador existente para uma senha conhecida. O módulo local somente pode ser executado pelo usuário root e possui o seguinte nome: **`/etc/firewall/fwadmin`**.

Interface texto

Eu estou trabalhando com a interface texto e reparei que ela não mostra os acentos de nenhuma palavra. Por que isso acontece ?

Ao escrever a interface texto, nos optamos por não utilizar acentos, em virtude de existirem vários tipos de terminais e de páginas de código diferentes, o que poderia provocar o aparecimento de caracteres estranhos em muitos terminais.

Além disso, seria muito incômodo para o usuário se as opções fossem exigidas com acentos (por exemplo, ter que se digitar *depuração* ao invés de *depuracao* na hora de se escolher a prioridade para se filtrar log ou eventos).

Criptografia

Estou configurando um canal seguro entre dois Firewalls Aker, um com a versão 3.01 e outro com a versão igual ou superior a 3.10. Configurei troca de chaves via SKIP e coloquei o mesmo segredo compartilhado em ambos os firewalls, entretanto recebo mensagens de *Pacote não passou pela autenticação* todas as vezes que tento fazer os dois se comunicarem. O que está errado ?

A versão 3.10 do Firewall Aker sofreu alterações em alguns pontos do algoritmo SKIP, devido a problemas de compatibilidade com outros sistemas operacionais, e o tornou incompatível com as versões anteriores.

A solução para este problema é atualizar todas as versões anteriores à 3.10 para a 3.10 ou superior (que são totalmente compatíveis entre si).

SNMP

Reparei que quando administro o Firewall Aker na plataforma Linux, as comunidades de leitura e escrita SNMP, da janela de parâmetros de configuração, se encontram desabilitadas. Por que isso acontece ?

O sistema operacional Linux já vem com um agente SNMP pré-instalado. Desta forma, optou-se por não instalar o agente SNMP do Firewall Aker.

Para aprender como configurar as comunidades de leitura e escrita do agente SNMP do Linux, consulte sua documentação.

Serviços Diversos

Como configurar os Servidores de Correio MS Exchange para funcionar através do Firewall Aker ?

Para possibilitar o correto funcionamento dos servidores Exchange através de firewalls é necessário a fixação das portas a serem utilizadas por estes servidores. Para fazer isso, é necessário a inclusão das seguintes chaves no registry dos servidores (todas as chaves são case-sensitive):

Em
`HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeMTA\Parameters`
Acrescentar a DWORD TCP/IP port for RPC listens com o valor da porta a ser utilizada (por exemplo, 30001).

Em
`HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeSA\Parameters`

Acrescentar a DWORD TCP/IP port com o valor da porta a ser utilizada (por exemplo, 30002)

Em
`HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeDS\Parameters`
Acrescentar a DWORD TCP/IP port com o valor da porta a ser utilizada (por exemplo, 30003)

Em
`HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\Parametersystem`
Acrescentar a DWORD TCP/IP port com o valor da porta a ser utilizada (por exemplo, 30004)

Obs1: Após feito o acréscimo destas keywords, deve-se reiniciar o servidor exchange.
Obs2: Caso a versão do Exchange seja a 5.5, é necessário a aplicação do Service Pack 2 ou superior do Exchange para que esta fixação de portas funcione.

Configuração do Firewall Aker para o funcionamento com a configuração descrita acima:
Para possibilitar o acesso ao servidor Exchange deve-se liberar as portas criadas nos itens anteriores (no exemplo acima 30001, 30002, 30003 e 30004) e a porta 135 (Windows RPC). Além disso, caso se esteja utilizando LDAP, deve-se liberar também as portas 389, para autenticação básica, e/ou 636, para autenticação SSL.

Como configurar o acesso ao gateway MS SNA Server ?

O gateway MS SNA utiliza as portas 1477/tcp e 1478/tcp para se comunicar, portanto estes serviços deverão estar configurados no Firewall Aker. Na configuração do Cliente SNA e na opção Advanced, certifique-se que todas as caixas de opção estejam desmarcadas e o nome do domínio NT de autenticação esteja preenchido.

Tenho um gateway MS SNA na rede interna de classe inválida e não consigo acessá-lo utilizando a conversão de endereços para o referido servidor ?

O MS SNA sempre retorna o número IP do servidor em que será feita a transação com o gateway a partir da porta 1478/tcp. É necessário que seja feita uma modificação no registro do cliente que está se utilizando.

Para alterar as configurações do registry de cada tipo de cliente, deverá ser modificado da seguinte forma:

No Windows NT:

1. Vá para a subtree HKEY_LOCAL_MACHINE na seguinte subchave:

System\CurrentControlSet\Services\SnaBase\Parameters\SnaTcp\

2. Adicione a seguinte informação: (todas as chaves são case-sensitive)

Value Name: FireWall

Data Type: REG_MULTI_SZ

Data: <Endereço IP da Conversão ou do Firewall Aker>

No Windows 95:

1. Vá para a subtree `HKEY_LOCAL_MACHINE` na seguinte subchave:

`Software\Microsoft\SnaBase\Parameters\SnaTcp\`

2. Adicione a seguinte informação:

Value Name: FireWall

Data Type: REG_SZ

Data: <Endereço IP da conversão ou do firewall Aker>

No Windows 3.x:

1. Adicione a seguinte informação no arquivo WIN.INI abaixo da seção [WNAP]:

[WNAP]

FireWall =<Endereço IP da conversão ou do firewall Aker>

Esta sendo logado a seguinte mensagem para a console do firewall:

xl3: transmission error: 90
xl3: tx underrun, increasing tx start threshold to 120 bytes
xl3: transmission error: 90
xl3: tx underrun, increasing tx start threshold to 180 bytes

Apareceu também para a xl0 e xl2. Alguma explicação ?

Estas mensagens são normais. Elas aparecem com alguma freqüência e não causam nenhum problema no funcionamento do firewall (na verdade o driver das xl e das de são muito *verbose* e produzem muitas mensagens que assustam o administrador sem necessidade).

Nas ações do Firewall existe a seguinte mensagem:
080 - Número de processos excessivo no sistema
e como solução está escrito:
Solução: Aumente o número máximo de processos no sistema.
Como podemos fazer isto no FreeBSD e Linux ?

No FreeBSD tem duas formas:

- Recompilar o kernel setando a opção maxusers para um valor maior (200,500, etc)
- Usar o comando sysctl, com a seguinte sintaxe (neste caso, deve-se aumentar o numero de processos e de descritores de arquivos, este ultimo deve ser duas vezes maior que o primeiro):

```
#sysctl -w kern.maxproc=xxxxx
#sysctl -w kern.maxfiles=2*xxxxx
```

No Linux só existe uma opção: recompilar o kernel. Nesse caso, deve-se aumentar a variável NR_TASKS para um valor maior (o Maximo é 8192 e o default é 512). Essa variável esta localizada no arquivo `/usr/include/linux/tasks.h`

Muitas vezes é necessário testar as máquinas por intermédio dos comandos tracert (do Windows) ou traceroute (nos Unix), para tanto como seria as configurações necessárias nas regras do firewall para que estes comandos possam ser executados e os resultados chegarem na máquina de origem ?

Para possibilitar que os pacotes de tracert ou traceroute tenham a passagem liberada no firewall faça o seguinte:

1. Cadastre a entidade Traceroute (serviço), englobando um intervalo de portas UDP entre 30.000 e 40.000
2. Crie regras habilitando a passagem dos pacotes de acordo com a configuração abaixo:

   Origem: Internet
   Destino: Rede a partir da qual se vai realizar o traceroute ou tracert
   Serviços: Echo Reply, Destination Unreachable, Time Exceeded.
   Ação: Aceita

   Origem: Rede a partir da qual se vai realizar o traceroute ou tracert
   Destino: Internet
   Serviços: Echo Request, Traceroute.
   Ação: Aceita

ATENÇÃO: O uso do intervalo de porta de 30.000 até 40.000 é necessário apenas para o traceroute (unix). O tracert não faz uso dessas portas.

Como faço para não registrar as informações de broadcast no log do firewall ?

Suponhamos que um firewall proteja as seguintes redes:

Rede 1 - 10.0.1.0/255.255.255.0
Rede 2 - 200.200.20.0/255.255.255.0
Rede 3 - 10.0.20.0/255.255.255.0

Para se evitar que os broadcast sejam registrados no log do firewall faça o seguinte:

1. Cadastre três entidades tipo máquina:
   Broadcast Rede 1 - IP 10.0.1.255

Broadcast Rede 2 - IP 200.200.20.255
Broadcast Rede 3 - IP 10.0.20.255

2. Crie uma regra, de preferência no início da Lista de Regras, de modo que fique da seguinte forma:

   Origem: Rede 1, Rede 2, Rede 3
   Destino: Broadcast Rede 1, Broadcast Rede 2, Broadcast Rede 3
   Serviços: Todos TCP Todos UDP Todos ICMP
   Ação: Descarta

Obs - Certifique-se que nenhuma opção do Log nos parâmetros da regra esteja marcado.

Muitas vezes temos de utilizar o cliente de correio Outlook 2000 (do pacote Office) para acessar as contas de correio que estão em um servidor Exchange, contudo o nome netbios é o usado por padrão nas configurações de clientes e na maioria das vezes a conexão originada da Internet não consegue resolver o nome netbios. Como resolver ?

O método mais fácil para não ter que ficar abrindo várias portas do firewall para resolução netbios é criar
um arquivo de nome <hosts> e colocá-lo do diretório c:\windows dos clientes.
Dentro deste arquivo deve ter o nome netbios do servidor e seu número IP. Exemplo exchange 200.200.20.35
Para verificar se o mesmo esta correto de um <ping exchange>, o qual será feita a resolução para o nome informado.

Compartilho o meu proxy SQUID do meu departamento com outros proxies também SQUID dentro da minha empresa, sendo o meu PARENT dos outros. O problema é que os proxies filhos não completam as requisições web. Todos os outros departamentos também são protegidos pelo Firewall Aker. Como resolver ?

O SQUID utiliza normalmente a porta 3128 para receber as transações web (ou outra que o administrador configurar), entretanto quando é formado uma array ou um parentesco entre os proxies SQUID, para melhor utilização dos caches, é necessário que seja liberado a transação de pacotes ICP na porta 3130. Estes pacotes levam as informações dos índices dos caches.

Para resolver o problema atente para os seguintes casos:

1. Caso o seu squid seja o pai e não haja registro nas suas configurações de quais são os filhos, basta apenas acrescentar na regra que libera o acesso ao proxy o serviço ICP (já cadastrado de fábrica)
2. Caso haja o registro de parentesco no seu SQUID (PARENT e SIBLING), devem existir regras permitindo o envio e o recebimento dos pacotes icp para as máquinas em questão.

Como enviar as mensagens do firewall para um pager via e-mail ?

1) Instale na sua máquina Firewall Aker os seguintes os pacotes tcl , tk e expect (caso não tenha instalado estes pacotes eles encontram-se no cd do FreeBSD no diretório

packages, no caso do linux eles estão no diretório RPM e iniciam com os mesmos nomes. Pode-se também montar o cd em um servidor ftp, só não esqueça de mudar para o modo passivo < passive> na linha de comando do cliente ftp estando dentro do firewall.
Obs: os sinais < > são apenas para delimitar os comandos ou variáveis

2) Baixando os pacotes em uma pasta de trabalho faça a instalação de cada um deles (atente para a ordem):

FreeBSD
pkg_add tcl.xx.xx.tgz
pkg_add tk.xx.xx.tgz
pkg_add expect.xx.xx.tgz

Linux
rpm -ivh tcl.xxxx.i386.rpm
rpm -ivh tk.xxx.i386.rpm
rpm -ivh expect.xxx.i386.rpm

Obs: os "xis" corresponde a versão dos pacotes.

3) Crie um arquivo de nome mobiaker com o seguinte conteúdo (Neste exemplo utilizo o serviço da mobitel)

----------Inicio do Script, Não Inclua esta linha----------
```
#!/usr/local/bin/expect
# este argumento é o tipo da mensagem do Aker que
# pode ser 1 - log ou 2 - evento
set tipo [lindex $argv 0]

# Prioridade (7 - depuração, 6 - informação,
# 5 - notícia, 4 - advertência ou 3 - erro)
set prioridade [lindex $argv 1]

# Número da mensagem que provocou a execução do programa
# ou 0 para indicar a causa não foi uma mensagem
set numero [lindex $argv 2]

# A mensagem propriamente dita
set msg [lindex $argv 3]

# número do pager do administrador do firewall
set pager "nnnnnnn"

# coloco o tempo máximo de espera para 3 minutos
set timeout 180

# inicio a transação com o servidor email da mobitel
# irei fazer a transação direta via telnet
spawn telnet mailhost.mobinet.com.br 25
```

```
# espero pela string de conexão do servidor
expect "220"

# Envio meu dominio
send "helo foo.com.br"

# espero pelo servidor
expect "250"

# Quem sou eu . . .
send "mail from:admin@foo.com.br\r"

# espero pelo servidor
expect "250"

# Para quem vai a msg. No caso da mobi todas vão para um usuário
# de nome pager e no assunto é colocado o número do mobi de destino
send "rcpt to:pager@mobinet.com.br\r"

# espero pelo servidor
expect "250"

# Mando o servidor se preparar para receber dos dados
send "data\r"

# espero pelo servidor
expect "354"

# As linhas a seguir irão montar o corpo do email
send "From: admin@foo.com.br\r"
send "Date: \r"
send "To: pager@mobinet.com.br\r"

# Aqui eu faço a composição do número do pager
# O sistema da mobi envia então somente o corpo
# do email para o pager
send "Subject: pager=$pager\r"

# um avanço de linha
send "\r"

# envio a mensagem propriamente dita
send "$tipo $prioridade $numero $msg\r"

# Finalizo a mensagem
send ".\r"

# Espero o servidor
expect "250"
```

Caio fora
send "quit\r"
----------Fim do Script, Não Inclua esta linha----------

4) No meu caso criei um usuário de nome "probe". Não esqueça de mudar a propriedade do diretório para tanto dê o seguinte comando:
<chown probe:probe /usr/probe>
obs --> o diretório /home/probe é apenas um link simbólico para o diretorio acima. Não esqueça de colocar o script neste diretorio. No linux a pasta do usuário fica mesmo em /home/probe, pois o mesmo não monta o link simbólico.

5) Abra a interface do firewall Clique em Configurações --> Ações --> Parâmetros.
No programa Externo coloque </home/probe/mobiaker> ou outro nome de arquivo ou diretorio que tenha colocado o script.
No usuário coloque <probe> ou outro usuário que tenha criado.
Escolha as ações que deseja mandar para o mobi.

6) Cuidado ! Verifique se o arquivo que contenha o script possui as permissões de acesso e se esta setado para ser executado, se não:

chmod +x mobiaker

chown probe:probe mobiaker

7) Este script também funciona para o Linux, somente mude a primeira linha para <#!/usr/bin/expect>

Como verificar se o sistema de arquivos do firewall foi alterado ?

1) Baixe o arquivo fcheck de http://sites.netscape.net/fcheck/fcheck.html

2) Verifique se o perl está instalado no seu sistema, se não pegue do cd e faça a instalação.
Para verificar se um pacote está instalado:
FreeBSD --> pkg_info perl
Linux --> rpm -q perl
Para instalar:
FreeBSD --> pkg_add perl.xxx.tgz
Linux --> rpm -ivh perl.xxx.i386.rpm

Obs - caso falte algum outro pacote, o próprio gerenciador de pacotes vai avisá-lo, portanto
anote os avisos dos pacotes que estão faltando e faça a instalação. Geralmente o linux e freeBSD já instalam o perl.

3) Desempacote o fcheck em algum diretório (o mesmo vem em FCheck_2.07.51.tar.gz ou FCheck_2.07.51.zip

4) Bem a partir daqui as modificações vão depender de cada um, ou seja os diretórios

escolhidos poderão ser outros, contudo tenha certeza de modificar os arquivos de configuração.Então aqui vão as minhas:
copie o arquivo <fcheck> para o diretório </usr/local/sbin>

5) Modifique o arquivo <fcheck> na linha que diz
<$config=/usr/local/etc/fcheck.cfg> (fica lá pela linha 153).
No meu caso copiei este arquivo <fcheck.cfg> para o dir <etc>, por isso minha linha ficou assim:
<$config=/etc/fcheck.cfg>

6) Crie uma pasta em /usr/local chamada <data>, desta forma:
mkdir /usr/local/data
É nesta pasta que será criada um banco de dados com os diretórios analisados.

7) Edite agora o arquivo <fcheck.cfg> para os diretórios que serão analisados. Observe que já tem um monte de exemplos. Eu particularmente coloquei os seguintes diretórios:
/bin, /sbin, /etc/, /lib/
Caso tenha a curiosidade de ler este arquivo, ele alerta para o fato de que se colocar o nome do dir mais a /, ou seja, /etc/ ele irá recursivamente analisar toda a árvore. Sem a barra ele somente fará a análise dos arquivos, excluindo os diretórios.

8) Existe no arquivo <fcheck.cfg> uma seção para excluir diretórios ou arquivos que não queira ser analisado, ou seja, supomos que tenha escolhido todo o /etc/ para ser analisado, contudo é feita frequentemente modificaçao no arquivo de regras do firewall, então coloque a seguinte linha:
Exclusion = /etc/firewall/conf/regras-350.filtro

9) Bem agora vamos rodar o programa para montar nosso banco de dados de arquivos, para tal de o comando:
/usr/local/sbin/fcheck -ca

10) Atente para o fato de que, qualquer alteração feita nos arquivos que vc está analisando terá de ser rodado novamente o comando acima. Para reforçar a segurança de o comando <ls -l> no diretorio <data> e anote a data e hora dos arquivos criados. No meu caso ficou assim:

```
[root@beicudo /etc]# ls -l /usr/local/data total 96
-rw-rw-r--   1 root     root         3906 Jul  1 23:54 beicudo.foo.com.br._bin
-rw-rw-r--   1 root     root        24650 Jul  1 23:54 beicudo.foo.com.br._etc_
-rw-rw-r--   1 root     root        61082 Jul  1 23:54 beicudo.foo.com.br._lib_
-rw-rw-r--   1 root     root         4889 Jul  1 23:54 beicudo.foo.com.br._sbin_
Press any key to continue...
```

11) Agora é hora de ativar o nosso guardião, e para facilitar as coisas vamos fazer um script para analisar os diretórios e enviar o resultado por email.

12) Crie um arquivo de nome <cheque> (de preferência no /usr/local/sbin), com o conteúdo abaixo:

----------Inicio do Script, não Inclua esta linha----------
```
#!/bin/sh
PATH=/usr/lib:/bin:/usr/local/sbin:/usr/bin

DATE=`date`

(echo "To: admin@foo.com.br"
echo "From: BEICUDO"
echo "Subject: Analise de Seguranca do BEICUDO em $DATE"
echo ""
fcheck -a) 2>&1 | /usr/lib/sendmail -t
```
----------Fim do Script, NÃO Inclua esta linha----------

13) Não esqueça de tornar esse arquivo executável, deste modo:
chmod +x cheque

14) Faça um teste para ver se o script está funcionando:
./cheque

--> deverá chegar um email na sua caixa postal como o exemplo:

```
PROGRESS: validating integrity of /bin
STATUS: passed...

PROGRESS: validating integrity of /etc/
STATUS: passed...

PROGRESS: validating integrity of /lib/
STATUS: passed...

PROGRESS: validating integrity of /sbin/
STATUS: passed...
```

15) Para finalizar faça este script rodar tantas vezes quanto você queira utilizando o crontab. De os seguintes comandos:
crontab -e
tecle i
digite <20 00 * * 0-7 /usr/local/sbin/cheque> # roda o comando todo dia à 00:20
tecle <:> e depois <wq> para gravar as configurações (crontab usa vi)

16) Pronto , o firewall agora possui mais uma ferramenta para evitar qualquer "surpresa".

Apêndice C - Copyrights e Disclaimers

Neste apêndice estão listados os *disclaimers* das bibliotecas e códigos fontes de terceiros utilizadas no Firewall Aker. Estes *disclaimers* se aplicam apenas às partes explicitamente citadas e não ao Firewall Aker como um todo. Eles estão citados aqui devido a exigências das entidades desenvolvedoras:

Biblioteca DES

Copyright (C) 1995 Eric Young (eay@mincom.oz.au)
All rights reserved.

This library and applications are
FREE FOR COMMERCIAL AND NON-COMMERCIAL USE
as long as the following conditions are aheared to.

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this code is used in a product, Eric Young should be given attribution as the author of the parts used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by Eric Young (eay@mincom.oz.au)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence
[including the GNU Public Licence.]

Biblioteca de criptografia libcrypto

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE

GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Biblioteca SNMP

Copyright 1997 by Carnegie Mellon University
All Rights Reserved
Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Códigos do FreeBSD

Copyright (c) 1982, 1986, 1993
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Algoritmo MD5

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Agente SNMP

Copyright (c) 1996,1997 Wes Hardaker and the University of California at Davis

COPYRIGHT

Many portions of the code in this package were distributed by Carnegie Mellon University.
All other code and changes to the original code written by Wes Hardaker at the University of California at Davis is copyrighted under the following copyright:

Permission is granted to use, copy, modify and distribute this software and documentation. This software is distributed freely and usage of it is not subject to fees of any kind. It may be included in a software compact disk set provided that the author is contacted and made aware of its distribution.

Biblioteca de números extendidos LInteger

LInteger Version 0.2 Source Code and Documentation

Copyright (C) 1996 by Leonard Janke

This source code and documentation may be used without charge for both commercial and non-commercial use. Modification of the source code or documentation is allowed provided any derivate work is clearly indentified as such and all copyright notices are retained unmodified. Redistribution of the source code or documentation is unlimited, except by the limits already mentioned, provided that the redistribution is not for profit. Those wishing to redistribute this source code or documentation or any work derived from either for profit must contact Leonard Janke (janke@unixg.ubc.ca) to work out an acceptable arrangement.

Anyone who wishes to distribute a program statically linked against the functions provided may do so providing that he or she includes a copy of this note with the program.

Distribution of libraries compiled from this source code is unlimited if the distribution is not for profit and this copyright notice is included. Those wishing to distribute libraries compiled from this source code or any work derived from it for profit must contact Leonard Janke (janke@unixg.ubc.ca) to work out an acceptable arrangement.

Anyone using this source code or documentation or any work derived from it, including, but not limited to, libraries and statically linked executables, must do so at his or her own risk, and with understanding that Leonard Janke will not be held responsible for any damages or losses that may result.

Apêndice D - Novidades da Versão 5.0

Neste apêndice estão listadas as principais alterações e novidades da versão 5.0 quando comparada à 4.5.

- Interface gráfica de administração multiplataforma e totalmente reescrita;
- Possibilidade de se administrar diversos firewalls simultaneamente através da mesma interface;
- Cluster cooperativo, com a possibilidade de uso de até 64 firewalls em paralelo dividindo o tráfego entre eles. Neste tipo de cluster não há perda de conexões, mesmo no caso de queda de um ou mais dos firewalls participantes;
- Balanceamento de links, possibilitando o uso simultâneo de diversos links de provedores de acesso (distintos ou não);
- Proxy SMTP com mais funcionalidades;
- Detecção e remoção de vírus nos downloads HTTP e FTP;
- Controle de anti-spoofing aperfeiçoado, não sendo mais feito em cada regra;
- Suporte ao protocolo 802.1q;
- Suporte aos protocolos RADIUS e LDAP para autenticação de usuários;
- Agrupamento de regras de filtragem em políticas;
- Perfis de acesso hierárquicos;
- Mecanismo de proteção anti-suicídio;
- Visualização de estatísticas do uso de CPU e memória da máquina onde o firewall está rodando através da interface gráfica em tempo real;
- Controle anti-flood, limitando o número máximo de conexões originadas em uma determinada máquina para um determinado serviço/servidor